EUROPEAN REVIEW OF DIGITAL ADMINISTRATION & LAW

VOLUME 3
ISSUE 2
2022

DATA GOVERNANCE, OPEN DATA AND DATA PROTECTION IN THE PUBLIC SECTOR

aracne

ERDAL

European Review of Digital Administration & Law / Erdal – *biannual review*

Submitting manuscripts
Manuscripts should be submitted via email to info@erdalreview.eu
For any queries on submission guidelines and procedures, please contact the Review.

Citation format
Editorial rules can be downloaded from the Review website.

Peer review procedure
This journal uses a double-blind review model.

Subscriptions
For subscriptions please contact: info@adiuvaresrl.it

Responsible Director: Angelo Giuseppe Orofino. Review registered at no. 12 of press register of the Court of Bari on 15 July 2020.

European Review of Digital Administration & Law

2022
Volume 3
Issue 2

ERDAL

This volume is part of the research project "Open data and re-use of public sector information in the context of its digital transformation: adapting to the new EU legal framework", funded by the Spanish Ministry of Science and Innovation (MCIN/AEI /10.13039/501100011033)

aracne

ISBN
979-12-218-0798-1

I^ST EDITION
ROMA 31 MARCH 2023

TABLE OF CONTENTS

Monographic Section: *Data Governance, Open Data and Data Protection in the Public Sector*

(eds. Fabio Bravo and Julián Valero Torrijos)

Studia Varia

Case Analysis

National Reports

Book Review

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 5-8
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 01

Data in the Public Sector and Data Valorisation

Fabio Bravo and Julián Valero Torrijos

1. *Legal Issues relating to Data in The Public Sector and The Process of Technological Modernisation Through the Lens of Data Valorisation*

The analysis of legal issues relating to data in the public sector covers several topics, all of which are of particular relevance, both on their own and as part of a global vision, leading to the identification of (i) the new set-up of public-private relations, (ii) the new balance between public powers and citizens' rights, (iii) the emergence of new duties for public sector bodies and new rights for individuals and companies, (iv) the new role of public administration in the data-driven society and economy. Looking at the phenomenon from another perspective, these are issues that highlight the new dimension of *data valorisation*, which poses new questions and new challenges to jurists and scholars.

The process of technological modernisation that has been taking place in the public sector throughout Europe in recent years poses a major challenge to the parameters within which the academic debate in the field of Public Law has been taking place. It can even be argued that there is a latent tension between the parameters on which the Public Administration is conceptually based and the demands of adaptation to change, innovation and learning capacity that are required today.

From a legal point of view, the important challenges facing European society have been highlighted by the assertion that it is essential to rely on a clear legal environment that encourages innovation and facilitates fairness and balance between the various actors involved. However, the legal guarantees on which regulation and its doctrinal analysis have traditionally been based have not kept up – at least not with the necessary agility and intensity – with the dizzying pace imposed by technological innovation.

In many cases, the fashion for technological innovation only presents us with mere labels imposed by advanced marketing and communication strategies. On the other hand, however, we are witnessing a paradigm shift that should be the object of greater legal attention, particularly in terms of academic analysis. Otherwise, we may find that technological innovation ends up dazzling us and prevents us from perceiving the changes that are actually taking place, so that legal guarantees frequently become a burden and are therefore undervalued in their true value; or even that we fail to notice their actual importance in an ecosystem of continuous innovations that only consider the limits of technology as their only limit, turning the Law into a lesser evil that has to be complied with only from the point of view of mere formalism.

2. *New Scenarios in The Age of Datification and New Roles for Public Administrations within the "European Strategy for Data"*

Globalisation has led to a crisis in the sovereignty of nation-States and to new and multiple forms of 'digital sovereignty',[1] in the face of which new dynamics in the relationship between the public and private spheres are emerging.[2] The processes of identification and recognition of the identity of individuals also take on new connotations in the digital environment,[3] in which the action of the nation-State – in the field of digital identity – appears recessive compared to the role played by the large private companies, which manage services and technological infrastructures, including data platforms, on a planetary level.[4]

[1] L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy & Technology*, 2020, 33, 369–378.

[2] See L. Cluzel-Métayer, C. Prébissy-Schnall and A. Sée (eds.), *La transformation numérique du service public: une nouvelle crise?*, Paris, Mare & Martin, 2021; A.G. Orofino, *La solidarietà in diritto amministrativo: da strumento di protezione dell'individuo a parametro di disciplina del rapporto*, in *Il diritto dell'economia*, 2020, 2, 571-598.

[3] G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 2017, vol. 33, 3, 723-727; G. Finocchiaro, *Identità personale (diritto alla)*, in Vv.Aa., *Digesto delle Discipline Privatistiche*, Torino, Utet, 2010, 721-738.

[4] J. Eynard (ed.), *L'identité numérique - Quelle définition pour quelle protection ?*, Bruxelles, Larcier, 2020.

In this scenario, the public administration has long been called upon to play a new role, which has recently been outlined with decidedly innovative features in the new European legal framework on data governance, open data and data spaces.[5]

The public administration now also acts as a data intermediary and facilitator in the circulation of the personal and non-personal data it holds, ensuring that such data can be reused by data users for commercial and non-commercial purposes.[6] These aspects have to be balanced with the right to personal data protection, in a delicate balance of interests that is not always easy to reconcile.

In the new technological context, that of the pervasive transition to digital technologies based on the massive use of data (with an impact that is unprecedented in history),[7] we are experimenting with new directions, which lead us to take untrodden paths, without knowing whether the point of arrival is a harbinger of advantages or disadvantages.[8]

Some fears are becoming more and more substantial, including, for instance, those about the risks arising from the use of artificial intelligence, the excessive centralisation of data in the hands of a few parties, mass surveillance, data manipulation, progressive loss of freedom, exposure to the inhuman logic of the algorithm.[9] Alongside the fears, however, deep hopes are nurtured for a significant improvement in economic and social conditions, benefiting the community as a whole, as well as individuals, due to the advantages of using the vast amount of data available today.

In this perspective, the discourse on the valorisation of data emerges strongly and presents us with new challenges that we should be able to grasp. The increasing datafication of society, economy and institutions is a phenomenon that is now well established and is at the centre of important strategic choices of both the EU and nation-States (also in relation to other strategic choices made by third countries, such as the United States and China). The current scenario sees the majority of personal and non-personal data concentrated in the hands of a few Big Players, mostly private multinational companies, of US origin, operating in an oligopoly regime, if not a substantial monopoly, as it is sometimes the case if we consider specific services.

The European Commission, in its 2020 Communication on "*A European Strategy for Data*",[10] estimated that 80 per cent of data are centralised on the servers of major ISPs and the remaining 20 per cent are decentralised within citizens, companies and institutions. However, the European Commission predicted that by as early as 2025 the situation could be reversed, with 80 per cent of data controlled and managed at the peripheric level by those who produce the data (i.e. citizens, businesses and institutions) and only the remaining 20 per cent remaining on the central servers managed by ISPs. According to the European Commission, this paradigm shift will be driven by several factors, such as (i) a significant increase in the volume of data 'produced' by citizens, businesses and institutions; (ii) the development of new technologies and new products and services based on data, which may lead to greater control by the new 'producers' of data.

Therefore, a significant overturning of data business models is expected, with the possibility of disrupting the current oligopolistic centralisation in the management of data-related services, currently concentrated in a few ISPs. To enable this,

[5] J. Valero Torrijos, *Datos abiertos y reutilización en el contexto de la Estrategia europea de datos*, in *Tábula*, 2021, 201-213; G. Resta, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 4, 971-995.

[6] F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, 199-256; D. Poletti, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, 46-51.

[7] J.-B. Auby, *Administrative Law Facing Digital Challenges*, in *Erdal*, 2020, Vol. 1, Issue 1-2, 7-15.

[8] See, for instance, H. Gimpel and F. Schmied, *Risks and Side Effects of Digitalization: a Multi-Level Taxonomy of the Adverse Effects of Using Digital Technologies and Media*, in *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden, 2019; D. Lupton, *Digital risk society*, in A. Burgess, A. Alemanno and J.O. Zinn (eds.), *Routledge Handbook of Risk Studies*, Oxon-New York, Routledge, 2016, 301-309; M.U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 in *Harvard Journal of Law & Technology*, 2016, 29, 2, 353-400; A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in *Erdal*, 2020, Vol. 1, Issue 1-2, 63-67.

[9] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, Laterza, 2014.

[10] European Commission, *A European Strategy for Data*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2020/66 final.

however, it is necessary to review the rules on the governance of data, which is necessary for their exploitation, whether they are in public or private hands.

3. *The (Polysemic) Value of Data*

This paradigm shift is part of the European Commission's aforementioned Communication, which aims to implement a new strategy for the valorisation of data in an anthropocentric and value-oriented perspective that does not renounce the protection of individuals and their fundamental rights, without neglecting the opportunities for citizens, companies and institutions.

What stands out in this discourse is the recognition of the value of data, where 'value' and 'valorisation' are polysemic terms that do not necessarily have an economic connotation:

(i) with reference to personal data, they constitute a 'value', first and foremost, because, in application of the personalistic principle, they represent aspects of the personality of the individual to whom they refer and, therefore, are attributes of the person and expressions of all that is linked to that person;

(ii) in another respect, it is well known that data have economic value, but it is important to bear in mind that the economic value of data does not exist in itself. It exists because of their use. In other words, it is not the personal data (*ex se*) that have economic value, but it is the processing of the personal data (i.e. the set of operations that can be performed with these data) that enables the user to derive economic benefit from the personal data. Personal data can be processed by data controllers only for a limited period of time and for a specific purpose, therefore personal data are not owned by data controllers and are not the property of data controllers. Data controllers do not own the personal data they process. Data controllers only have the right to use them for a limited period of time and for a specific purpose, provided there is a legal basis – such as the consent of the data subject or another legal basis – under Articles 6 and 9 of the GDPR. They have the right to use them, also for economic purposes, but this right is not a property right.[11] Attempts to reify and frame personal data as a legal good to be sold or traded are not allowed in the European legal system. Obviously, the temporary availability of personal data held by data controllers for specific purposes allows data controllers to provide services based on such data within the scope of those purposes;

(iii) however, data also constitute value in other senses: their processing enables the attainment of the purposes intended by the data controller, so that they carry within themselves the value expressed by those purposes. In this perspective, the value of the personal (and non-personal) data is equal to the value that the data controller would achieve through processing of the data. This value could be economic and non-economic;

(iv) again, data enable the achievement of a public interest and a relevant public interest within the meaning of Articles 6(1)(e) and 9(2)(i) GDPR. Thus, the valorisation of data, especially when processed by public authorities, is linked to the realisation of such "public interest", understood as the good and interests pursued by the actions of public sector bodies for the benefit of the community;

(v) the value of personal and non-personal data can be extended in an ultra-individual (ultra-egoistic) direction even when the processing is carried out by private parties, who may direct the data to be processed to fulfil altruistic purposes. This is constantly the case, for example, when processing is carried out by non-profit organisations, such as associations and foundations, but it can also be the case when the altruistic interest is pursued by a party, including the data subject, who wishes to make available the data they have in order to satisfy interests that go beyond those relating to himself or herself, by altruistically pursuing the satisfaction of interests relating to other parties (*data altruism*);

(vi) finally, the European Commission stressed another aspect that is directly linked to technological development: processed data, both personal and non-personal, are useful – and this is where they have an enormous value – also in an instrumental sense, because they make it possible to take more efficient, more targeted and sometimes even personalised decisions. The use of data to support decision-making – through automated decision-making

[11] F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, Wolters Kluwer-Cedam, 2019.

processes – is certainly another relevant aspect to be taken into account in the perspective of data valorisation, which is also often used by public authorities (and which may also involve significant disadvantages for the data subject, if the automated decision has a negative impact on his or her person or infringes on his or her fundamental rights and freedoms).

It should be noted that for a full valorisation of data, especially by public administrations, it is extremely important to establish common *European Data Spaces* in the EU, in all strategic societal sectors and domains of public interest. According to the European Commission's Communication on "a European strategy for data", Data Spaces are envisioned as sovereign, trustworthy and interoperable data sharing environments where data can flow within and across sectors, in full respect of data subjects' fundamental rights and interests.

4. *From Data Protection to Data Governance*

To this end, a coherent, global and systematic treatment is essential for overcoming the fragmentation and biases that have been detected up to now. Even more, this perspective will make it possible to provide appropriate answers, specific to the technological field in which challenges arise.

From the perspective of document management, technological modernisation entails a consequence that cannot be underestimated from the perspective we are dealing with here: it is not enough to limit oneself to a mere change in the medium and simply replace the management of paper documents with their electronic equivalents. Indeed, the advanced use of electronic means requires data to be detached from the original document in which they may be contained and thus to be processed independently.

In this respect, automation allows greater possibilities for information use and, above all, demands efficiency in administrative action to overcome this model since data revolution represents a major opportunity for management to improve the public sector.[12] Thus, information must be generated by design and by default in a format that allows its subsequent automated processing based on the submission to interoperability standards that, in short, facilitate its use for purposes other than those that initially justified its collection and processing. The importance of data in this context makes it essential to face the restrictive inertia that, both at doctrinal and practical levels, implies an absolute pre-eminence of an excessively-formalistic vision of personal data protection.

In short, the data held by the public sector – and those generated, managed and handled by private parties linked to it – are becoming a tool of great significance in the process of digital transformation that is currently being experienced. Consequently, the adaptation of the regulatory framework to the challenges and singularities it implies not only is imperative but urgent as well. To this end, it is essential to move from data protection to data governance, a broader and more flexible approach that, necessarily and from the perspective of the European Union model, must be based on the effective respect for fundamental rights and public freedoms… including personal data protection.

[12] S. Goldsmith and S. Crawford, *The responsive city. Engaging communities through data-smart governance*, San Francisco, Jossey-Bass, 2014, 118.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 9-12
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 02

*Data and Digital Sovereignty**

Giusella Finocchiaro
(Full Professor of Private Law and Internet Law at University of Bologna)

ABSTRACT The Author examines the European strategy aimed at establishing a "digital sovereignty" based on European fundamental rights and values, by contrasting the recent dominance of private powers in the regulation of new virtual spaces. Nowadays times have changed, and public power needs to reclaim its role in the regulation of virtual life in a framework where there are multiple levels of rules which correspond to as many expressions of power. Especially the European Union should adopt appropriate legal instruments in order to affirm its leadership towards China and U.S.A.

1. *Data and digital sovereignty: the European approach*

Data are essential in the current economic scenario. They are definitively one of the newest and most interesting resources from an economic point of view, while the corresponding legal framework is going to be defined.

The expression "digital sovereignty"[1] has been widely used since at least 2020 when the European Commission President Ursula von der Leyen stated in the EU State of the Union address that: "it is about Europe's digital sovereignty, on a small and large scale".[2]

Europe, as we know, is not a technology producer and does not host any digital-communication platforms or systems of significance.

The European strategy has been to shift the playing field from technology towards rules. Therefore, within the geopolitical context the European Union's strategy is to present itself as a leader rulemaker and to ensure that the European model becomes a global standard and can be adopted within other geopolitical regions (the so-called "Brussels effect").[3]

The aim is not to compete with China and the United States in terms of technological production, but rather in terms of rulemaking. The goal is to assert European "digital sovereignty", which has both an external aspect in being projected towards the other two global actors, as well as an internal effect on the European Member States. The aim is on the one hand to establish a new model and on the other hand to avoid fragmentation.

For example, according to the explanatory memorandum accompanying the proposal for a Regulation on artificial intelligence,[4] "[i]t is

* Article submitted to double-blind peer review.
Where text is cited from a publication in a language other than English, the version of the citation provided in English is an unofficial translation by the author.

[1] There are many definitions of digital sovereignty. For L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Phil. & Tech.*, 2020, pp. 369-378, digital sovereignty essentially means control over digital affairs: "digital sovereignty, that is, for the control of data, software (e.g. AI), standards and protocols (e.g. 5G, domain names), processes (e.g. cloud computing), hardware (e.g. mobile phones), services (e.g. social media, e-commerce), and infrastructures (e.g. cables, satellites, smart cities), in short, for the control of the digital. Let me clarify that by 'control' I mean here the ability to influence something (e.g. its occurrence, creation, or destruction) and its dynamics (e.g. its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence. In this sense, control comes in degrees and above all can be both pooled and transferred" (pp. 370-371). In particular, "Sovereignty is a form of legitimate, controlling power (…) we can now qualify as national sovereignty the controlling power exercised by the State on its territory, on the resources that are found in it, and the people who live there. The digital age is forcing us to rethink the nature of sovereignty. But who should exercise it de facto and de jure?" and "Today, the fight is not over secular and spiritual power but over corporate and political power over the digital" (p. 372 and p. 377). F. Casolari, J. Cowls, L. Floridi, J. Morley, H. Roberts and M. Taddeo, *Safeguarding European values with digital sovereignty: an analysis of statements and policies,* in *Internet Policy Review,* 2021, consider digital sovereignty as "authority over the digital" (p. 2) and more specifically "a form of legitimate, controlling authority" (p. 6). T. Christakis, *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, *e-book*, 2020 distinguishes between "sovereignty as regulatory power; and, sovereignty as strategic autonomy", as well as L. Moerel and P. Timmers, *Reflections on Digital Sovereignty,* EU Cyber Direct: Research in Focus, 2021.

[2] State of the Union Address by President von der Leyen at the European Parliament Plenary of 16 September 2020.

[3] On this issue, see generally A. Bradford, *The Brussels Effect: How the European Union Rules the World*, New York, Oxford University Press, 2020.

[4] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 21 April 2021, COM(2021) 206 final.

in the Union interest to preserve the EU's technological leadership.[5] However, the EU does not have any technological leadership in the field of artificial intelligence, as it is not one of the largest global producers.[6] On the contrary, as it is clarified in the Memorandum,[7] the goal is to "protect the Union's digital sovereignty and leverage its tools and regulatory powers to shape global rules and standards" which has been the stated objective of the President of the European Commission since she took up office.

2. *The European legislation*

This once again confirms the strategic design of European lawmakers, whose ultimate purpose in this case is to build a single European digital market, the normative structure of which is fundamentally expressed in four areas: first of all data protection, through the GDPR, and the exploitation of data provided for under the Data Act,[8] the Data Governance Act[9] and the proposal for a regulation on the European Health Data Space;[10] secondly digital services and the digital market, through the Digital Markets Act[11] and the Digital Services Act[12]; thirdly, as regards digital identity, through the review of the eIDAS Regulation from 2014;[13] and finally the proposal for a regulation on artificial intelligence, alongside the recent proposal for a "directive on adapting non-contractual civil liability rules to artificial intelligence" (AI Liability Directive).[14]

This model safeguards not only fundamental rights[15] but also European "values", a term that is also cited a number of times in the above-mentioned proposals, stressing that the proposed model is not only normative but also cultural. The aim is to make it clear that it is not only legal rules that are at stake, but also the culture that those rules express.[16]

3. *The need for public authorities to reappropriate normative space*

At the beginning, in the 1990s, Internet was ruled by private regulation, meaning contract rules, and technical rules. It was governed by *lex mercatoria* and by *lex informatica*.

Both were provided by private actors: commercial entities and technical entities. They were not stated by the legislators.

The situation has changed in various respects since the 1990s, and public authorities have reclaimed a role for

[5] See p. 1 of the Memorandum.

[6] According to a recent report by the European Investment Bank, there is an investment gap of 10 billion euros in the EU in the area of AI and blockchain technologies. "80% of global annual investments in these technologies are concentrated in the USA and China, whilst Europe invests only 7% of the total". See N. Serri, *L'Europa in ritardo: politica industriale e diritti*, in *Aspenia*, 2021, 247.

[7] See p. 7 of the Memorandum.

[8] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM (2022) 68 of 23 February 2022, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN.

[9] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[10] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022)197.

[11] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), published in the Official Journal of the European Union L 265/1 of 12 October 2022.

[12] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), published in the Official Journal of the European Union L 277/1 of 27 October 2022.

[13] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No. 910/2014 as regards establishing a framework for a European Digital Identity, 3 June 2021, COM(2021) 281 *final.*

[14] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 of 28 September 2022.

[15] The following rights enshrined in the Charter of Fundamental Rights of the European Union are expressly referred to: human dignity (Article 1), respect for private and family life and protection of personal data (Articles 7 and 8), non-discrimination (Article 21) and equality between men and women (Article 23).

[16] On the comparison between Europe and the USA, see O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet*, Oxford, Hart Publishing, 2021. For an analysis of the similarities and differences between the respective approaches taken in China and the European Union in relation to sovereignty in cyberspace, see: Y. Chan Chin and K. Li, *A Comparative analysis of Cyber Sovereignty Policies in China and the EU*, paper presented at the TPRC 2021, 49th *Annual Research Conference on Communications, Information, and Internet Policy*, September 2021. Digital sovereignty is also considered by A. Chander and H. Sun, *Sovereignty 2.0*, Georgetown Law Faculty Publications and Other Works, 2021, as well as G. Finocchiaro, L. Balestra and M. Timoteo (eds.), *Major Legal Trends in the Digital Economy*, Bologna, Il Mulino, 2022.

themselves within the "new spaces".

The scenario has changed as regards at least three aspects, which are – indeed – different manifestations of one and the same aspect: the greater significance of the digital domain, not only in economic terms, but also in social and political ones.

First and foremost, since the end of the 1990s our lives have increasingly shifted into the digital world. To use Floridi's evocative expression, we are living in the *onlife*.[17] Whereas until a few years ago a distinction was often drawn between the "real" and the "virtual", today this distinction no longer makes sense.

Perceptions of both individuals and society as a whole have changed, with the digital realm being increasingly regarded as an integral part of each individual's very existence.

In parallel, it is difficult to identify cause and effect, and opportunities for living one's life in the digital world have grown: from e-commerce, through social networks to online platforms.

Information has become entified and reified. It has become a "thing".

Data, whether personal or not, have become an object to be communicated and also exploited, constituting an asset that can be shared and exchanged. As it is known, a major recent development in artificial intelligence has also emerged out of, amongst other things, the level of access to data that is nowadays possible.

Finally, the role of the major digital actors who create the conditions for *onlife* interactions and architecture, has grown. They are now not only actors but also directors. Indeed, they are also producers of the *onlife*, if one considers their economic weight, thanks to the value that data and information have now taken on.

In summary, the digital world has morphed from a niche first occupied at the dawn of the Internet by the military and academia into e-commerce and later into a pervasive aspect of society as a whole.

This has come as a shock for public authorities.

The *Trump* case was emblematic of the change. On 8 January 2021, Twitter blocked the profile of the then US President due to the violation of Twitter's contractual terms, including specifically the risk of incitement of violence.[18]

This decision was extremely controversial. However, it can lead us towards different conclusions depending upon whether it is considered from a private law or a public law perspective.

If viewed in strictly contractual terms, Twitter acted properly, applying the terms of the contract. Where a user acted in a particular manner, Twitter had the right to suspend the account.

If by contrast the very same decision is viewed through a public-law lens, it may be seen to raise critical issues as regards the principle of freedom of information. However, this aspect does not concern relations between two private persons (a company and its customers), but rather the broader public dimension of the issue (a politician expressing his views).

After the Twitter profile of the then US President was cancelled, the problem was brought into sharp relief. The question arose as to whether contractual terms and private-law rules were sufficient, or whether by contrast relations with a potential public significance should be governed differently. In other words, should the legal model for mediating between different interests be revisited where a public interest is at stake (communication, information, fake news)? If a new approach needs to be followed, it must be established whether the legal remedy available under national law is sufficient, as well as which forms of international cooperation are practicable.

[17] L. Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era, Springer Nature*, Cham, Springer, 2015.

[18] Twitter announced as follows: "After close review of recent Tweets from the @realDonaldTrump account and the context around them — specifically how they are being received and interpreted on and off Twitter — we have permanently suspended the account due to the risk of further incitement of violence. In the context of horrific events this week, we made it clear on Wednesday that additional violations of the Twitter Rules would potentially result in this very course of action. Our public interest framework exists to enable the public to hear from elected officials and world leaders directly. It is built on a principle that the people have a right to hold power to account in the open. However, we made it clear going back years that these accounts are not above our rules entirely and cannot use Twitter to incite violence, among other things. We will continue to be transparent around our policies and their enforcement".

4. *Conclusions*

We are thus living in an age of "pluralism of sovereignty". A characteristic feature of this age is "not the absence of sovereignty, but rather that sovereignty is unbalanced, disconnected, disoriented and intermittent".[19]

After globalisation, during a period marked in any case by international interdependence and major disorientation, the aim is to establish a new architecture of power: supranational, State and private.

In the digital domain, the juxtaposition between public and private is clearly evident with respect to regulators and regulatory instruments.

On the one side there is the European Union and nation States, and on the other side the major corporations. On the one side there is the contract and the *lex mercatoria* and the *lex informatica*. On the other side, the legislation.

The regulatory power that, given the inertia on the part of public authorities, had previously been exercised by private bodies has now been reclaimed by public authorities, for reasons that we might define as the external and internal sovereignty of nation States.

This is because the matters to be regulated are no longer commercial but political. It is not only the market for e-commerce that is in play, but also the "market" for information and truth.[20]

We are thus living in an era of post-globalisation and international interdependence.

Ultimately, we will probably end up with a multi-level system in which a role will inevitably be performed by technology and contracts.

In future, at different levels, the international community, States and private actors will each make rules.

We are living through a period of change, moving towards an increasingly multi-level system.

Thus, if the matter to be regulated has become one that is of interest for the whole of society, and that has political significance, it is necessary for the political sphere to reappropriate its own role.

There is not an absence of rules, as it is often asserted with some degree of superficiality; on the contrary, rules are being proposed in large numbers that, considered in the abstract, could be applied to the various issues: this tangled mass needs to be sorted out in order to establish which rules should apply and how they can be coordinated with one another.

[19] See C. Galli, *Sovranità*, Bologna, Il Mulino, 2022, 124.
[20] A. Nicita, *Il mercato delle verità*, Bologna, Il Mulino, 2021.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 13-33
ISSN 2724-5969 – ISBN 979-12-218-0798-1 - DOI 10.53136/9791221807981 03

*Data Governance Act and Re-Use of Data in the Public Sector**

Fabio Bravo
(Full Professor of Private Law, University of Bologna, Italy; Director of the Postgraduate Course in Privacy and Data Protection Officer, University of Bologna, Italy)

ABSTRACT This article aims to provide a critical analysis of the legal framework for the re-use of data held by public sector bodies, in the light of both the European Commission's Communication on the European Data Strategy and the new European Data Governance Act. What emerges is a new approach by the European legislator that requires public administration to play a new role, not only as an intermediary and facilitator in the circulation of data, but also as the one who can 'empower' natural and legal persons to exercise their rights over data and information belonging to protected categories. The new protection mechanisms outlined in the Data Governance Act present significant critical aspects from a legal point of view, but also new perspectives, which are discussed in this work.

1. *A new European approach to data*

The European Commission, in its Communication entitled "A European Strategy for Data" [COM(2020) 66 final, 19.2.2020], has adopted a new fortified approach towards a regulation of personal and non-personal data. The starting point can be found in the awareness that "Over the last few years, digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans (…)."[1] In this scenario it was clearly stated that "(…) Data is at the centre of this transformation and more is to come. Data-driven innovation will bring enormous benefits for citizens, for example through improved personalised medicine, new mobility and through its contribution to the European Green Deal."[2]

On the basis of such premise, the European Commission significantly argued that "In a society where individuals will generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules."[3]

However, this anthropocentric vision also meets the needs of the (European single) market, in a multiple perspective typical of the European approach: together with the celebration of the individual protection of persons' fundamental rights and freedoms, we can find the statements concerning the opportunities of a relevant social and economic development.[4] In this direction, the Commission stated that "Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules. At the same time, the increasing volume of non-personal industrial data and public data in Europe, combined with technological change in how the data is stored and processed, will constitute a potential source of growth and innovation that should be tapped."[5]

The enormous significance attributed to the processing of (personal and non-personal) data can be perfectly understood. Data are openly considered "the new oil",[6] not without some negative implications which need to be addressed, especially in the field of data protection law[7], competition law[8] and AI law.[9] How-

* Article submitted to double-blind peer review.

[1] European Commission, *A European Strategy for Data* [COM(2020) 66 final, 19.2.2020], Brussels, 2020, 1.

[2] European Commission, *A European Strategy for Data*, 1.

[3] European Commission, *A European Strategy for Data*, 1.

[4] See also S. Rodotà, *Tecnologie e diritti*, Bologna, Il Mulino, 1995.

[5] European Commission, *A European Strategy for Data*, 1.

[6] K. Bhageshpur, *Data Is The New Oil - And That's A Good Thing*, in *Forbes*, 15 November 2019, available online at www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/;

[7] D.D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, in *Maine Law Review*, 2014, available at SSRN: https://ssrn.com/abstract=2393792; L. Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, in *Tennessee Law Review*, 2020, Vol. 85, available at SSRN: https://ssrn.com/abstract=3252543.

[8] See European Parliament, *Is data the new oil? Competition issues in the digital economy*, Brussels, 2020, available online at www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)6

ever, the main value of data should not be founded in their direct economic worth, but in the set of capabilities that can be derived from themselves, by means of an accurate analysis.
That is precisely the crux of the matter. The great value of data mainly consists in supporting decision-making. Data and data analysis allow for better decisions, with huge benefits for natural and legal persons, such as citizens, associations, foundations, non-governmental organizations (NGOs), enterprises and companies, and public administrations.
According to the above-mentioned Communication, "Citizens should be empowered to make better decisions based on insights gleaned from non-personal data. And that data should be available to all – whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident."[10]
The approach adopted by the European Commission seems not to be the one based on the "commodification" of personal and non-personal data, in order to have a monetary gain in the digital market of data, but the one that consider data as means of innovation and development for society, institutions and markets, both in private and public sector, "to enable the EU to become the most attractive, most secure and most dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all of its citizens."[11]
In fact, the European Union aims to build a different model, in which data do not consist in "commodities" or "goods", but, first of all, in "a value" available to all, as a key factor of growth, wealth and development, for the entire society, including citizens, public administrations, enterprises and other public and private bodies.
In this direction the European Commission strongly specified – in its Communication on "The European Strategy for Data" – that "The EU can become a leading role model for a society empowered by data to make better decisions – in business and the public sector. To fulfil this ambition, the EU can build on a strong legal framework – in terms of data protection, fundamental rights, safety and cybersecurity – and its internal market with competitive companies of all sizes and varied industrial base. If the EU is to acquire a leading role in the data economy, it has to act now and tackle, in a concerted manner, issues ranging from connectivity to processing and storage of data, computing power and cybersecurity. Moreover, it will have to improve its governance structures for handling data and to increase its pools of quality data available for use and re-use. Ultimately, Europe aims to capture the benefits of better use of data, including greater productivity and competitive markets, but also improvements in health and well-being, environment, transparent governance and convenient public services."[12]
A couple of years later, those considerations have been translated into a new regulation, dedicated to the European Data Governance: the EU Regulation No. 868/2022 ("Data Governance Act"),[13] by means of which the European legislator has intended to facilitate data-sharing in the internal market, by creating a harmonised legal framework for data exchanges, without prejudice to data protection law (Regulation No. 679/2016, General Data Protection Regulation – GDPR).[14]
Regarding that matter, the aim of this essay is to examine the legal framework and analyse the main disruptive legal issues concerning the governance of data held by public bodies under the above-mentioned Data Governance Act, focusing on the re-use of such data for commercial and non-commercial purposes and the new role attributed to the public bodies themselves, taking into account, at the same

46117_EN.pdf.
[9] G. Alpa, *L'intelligenza artificiale. Il contesto giuridico*, Modena, Mucchi, 2021; B. Custers and E. Fosch-Villaronga (eds.), *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice*, Springer, 2023; L. Floridi, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford, Oxford University Press, 2023.
[10] European Commission, *A European Strategy for Data*, 1.
[11] European Commission, *A European Strategy for Data*, para. 7.
[12] European Commission, *A European Strategy for Data*, 1.
[13] Regulation (EU) No. 868/2022 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). According to its Art. 38, the DGA is applicable from 24 September 2023.
[14] Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

time, the interrelations with the data protection law.

2. *Data Governance Act as a major component of the European Strategy for Data and the key role of data intermediaries*

It is perfectly clear, and it can be proved by the opening words used in the first Recital of the Data Governance, that the European legislator has intended to "provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted" and therefore "the development of a framework for data governance should contribute to the achievement of those objectives, while fully respecting fundamental rights."

The re-use of large amounts of personal and non-personal data held by public sector bodies is therefore, according to the European strategy, one of the main key factors in achieving this general objective, which is aimed at the development of a European data market, where competition is ensured, preserved, and facilitated. This approach is clearly outlined in the Data Governance Act, in which the European legislator wished to leverage and strengthen the role of relevant figures, capable of furthering this objective, both in the private and in the public sectors.

The fundamental idea underlying this strategy is to resort to public and private subjects as "intermediaries" of personal and non-personal data, so as to favour the movement and re-use of said data by other subjects, with various purposes, connected to the carrying out of entrepreneurial activities, for altruistic aims and to pursue a public interest.

It should be considered that Chapter III of the Data Governance Act (see Articles 10-15) contains the regulations of the "*Data intermediation services*"[15] provided by "*data intermediation services providers*",[16] which include not only private intermediaries that collect and facilitate the use of personal data belonging to others, but also "*data cooperatives*",[17] who obtain data from their own members and then circulate them in favour of other subjects,[18] and even public bodies: as is clearly noted by Recital No. 27, "Data intermediation services providers, which may include public sector bodies, that offer services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing."[19]

Data intermediation, within this framework, concerns commercial relationships, which the intermediary seeks to favour, even if they are a public sector body. Therefore Recital No. 29 DGA specifies, among other things, that "This Regulation should not apply to services of-

[15] In accordance with Art. 2, para. 1, no. 11, DGA, "'data intermediation service' means a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following:
(a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;
(b) services that focus on the intermediation of copyright-protected content;
(c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things;
(d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships."

[16] F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* 2021, 1, 199-256; D. Poletti, *Gli intermediari di dati*, in *European Journal of Privacy Law and Technologies*, 2022, 1, 45-56.

[17] F. Bravo, *Le cooperative di dati*, in *Contratto e impresa*, 2023, Vol. 39, Issue No. 3, 757-799; L. Petrone, *Il mercato digitale e le cooperative di dati*, in *Contratto e impresa*, 2023, Vol. 39, Issue 4, 800-817.

[18] The DGA, under Art. 2, para. 1, No. 15, expressly mentions the "services of data cooperatives", defined as "data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structure, having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data".

[19] The strategic importance of data intermediation services, offered by public and private sector subjects, is clearly highlighted in the rest of Recital No. 27, where it is added that "Data intermediation services are expected to play a key role in the data economy, in particular in supporting and promoting voluntary data sharing practices between undertakings or facilitating data sharing in the context of obligations set by Union or national law. They could become a tool to facilitate the exchange of substantial amounts of relevant data. (…)."

fered by public sector bodies in order to facilitate either the re-use of protected data held by public sector bodies in accordance with this Regulation or the use of any other data, insofar as those services do not aim to establish commercial relationships."

This seems like a way to counter the oligopoly (and in some cases the virtual monopoly) of extra-European "Big Tech" multinational corporations and favour both the rise of new European enterprises in this field, as well as of European data spaces, which are independent from those managed by the afore-mentioned multinational corporations and an alternative to them, with major effects on the market. The above-mentioned Recital No. 27 itself specifies that "(…) Specialised data intermediation services that are independent from data subjects, data holders and data users could have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power, while allowing non-discriminatory access to the data economy for undertakings of all sizes, in particular SMEs and start-ups with limited financial, legal or administrative means. This will be particularly important in the context of the establishment of common European data spaces, namely purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives. Data intermediation services could include bilateral or multilateral sharing of data or the creation of platforms or databases enabling the sharing or joint use of data, as well as the establishment of specific infrastructure for the interconnection of data subjects and data holders with data users."

Furthermore, under the Chapter IV of the Data Governance Act (see Articles 16-25) another kind of data intermediary – in a broad sense – has been regulated: the "recognised data altruism organisations", who have a role in the voluntary sharing of both personal and non-personal data, on the basis of the consent of data subject or permissions of data holders, without seeking or receiving any reward.[20] The Regulation does not use the term "intermediaries" for such entities, but it is perfectly clear that they operate in that very role, albeit in a different context and to meet other needs, other than commercial ones, to which *public administrations* are certainly not unrelated. One must but consider what is specified in Art. 16 DGA, which sets out that "Member States may have in place organisational or technical arrangements, or both, to facilitate data altruism. To that end, Member States may establish national policies for data altruism. Those national policies may, in particular, assist data subjects in making personal data related to them held by public sector bodies available voluntarily for data altruism, and set out the necessary information that is required to be provided to data subjects concerning the re-use of their data in the general interest."

Also to this end the Data Governance Act aims at achieving the EU's ambitious strategies in an innovative manner, by favouring the movement of data not only for market needs, but also for "altruistic" needs related to individual and social welfare, as well as for needs related to the pursuit of the general interest. A relevant element in this respect is the definition of "*data altruism*" contained in Art. 2, para. 1, No. 16, DGA, which states that it "(…) means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest."

What clearly emerges it the link between *data altruism* and *public administration*, whereby the personal data of the data subjects and the non-personal data of the data holders that are

[20] In accordance with Art. 2(16) of the Data Governance Act, "'*data altruism*' means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest."

voluntarily made available for altruistic purposes may be used by public sector bodies in the general interest, to improve the public policies and public services in the various sectors in which public administration operates, ranging from healthcare to mobility, from the environment to energy, as well as the activities aimed at preventing and tackling the consequences of climate change. The purpose of this list is simply to provide some examples and it may be enhanced in relation to every activity aimed at achieving the general interest, whose care is entrusted to the action of public administration.

Within the framework of data altruism, public administrations are not only considered subjects benefiting from the voluntary sharing of data by data subjects and data holders, provided for by Art. 2, para. 1, No. 16, DGA mentioned above. Broadly speaking, they themselves may act as intermediaries in the data altruism sector, by formally regaining the role of recognised *data altruism organisation* under Art. 18 of the Data Governance Act, which determines that "In order to qualify for registration in a public national register of recognised data altruism organisations, an entity shall: (a) carry out data altruism activities; (b) be a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, where applicable; (c) operate on a not-for-profit basis and be legally independent from any entity that operates on a for-profit basis; (d) carry out its data altruism activities through a structure that is functionally separate from its other activities; (e) comply with the rulebook referred to Article 22(1), at the latest 18 months after the date of entry into force of the delegated acts referred to in that paragraph."

Public administrations, owing to their role, are legal persons established under national law to pursue the general interests identified within the framework of the national law of a Member State (see lett. *b*) and, within this context, they operate without pursuing profit-making, independently from bodies seeking to pursue profit-making (see lett. *c*) by adopting an *ad hoc* "structure", tasked with performing these activities, in a manner that is functionally separate from the other institutional activities performed by the body (see lett. *d*), by complying with the "rulebook" adopted by the European Commission for the recognised data altruism organisations pursuant to Art. 22 DGA, through the adoption of delegated acts (see lett. *e*).

Thus public administrations could act more effectively in the field of data altruism, by entering a virtuous cycle functional to the pursuit of the general interest, with great potential in terms of efficiency increase and the good performance of public administration, all in compliance with the independence principle, which in the field under examination is also articulated based on subjects whose action is aimed at the pursuit of commercial and profit-making goals.[21]

Other specific rules concerning *public administrations as data intermediaries*, broadly speaking, are provided in Chapter II of the Data Governance Act (see Articles 3-9), dedicated to the "*Re-use of certain categories of protected data held by public sector bodies*."

The aim of this legal regime is to ensure that data, generated or collected by public administrations or other entities at the expense of public budgets, benefit the whole society, even though data, because of the special category which they pertain to, are out of the application of the EU Directive 2019/1024 on "*Open data and reuse of public-sector information*".

Therefore this aspect is also highlighted for the Data Governance Act, which is crucial to the free movement of data. The data held by public administration cannot be considered data owned by public administration to be used for its own benefit to perform sovereign powers, but rather as data of the community, which the public administration holds on behalf of the citizens, so as to pursue the general interest and as these data are collected and managed with economic resources taken from society, said data must be made available to society and, therefore, also to private citizens intending to pursue commercial and non-commercial purposes, not related to the initial purposes for which the data are acquired and processed by the public administration itself.

In this respect the content of Recital No. 6 DGA is far too clear, where it is clarified that "The idea that data that has been generated or collected by public sector bodies or other entities at the expense of public budgets should benefit society has been part of Union policy

[21] A good performance and impartiality of public administration are principles that in Italy are also set under Art. 97 of the Constitution: "(…) Public offices are organised according to the provisions of law, so as to ensure the efficiency and impartiality of administration (…)."

for a long time (…)", as is the content of Art. 2, para. 1, No. 2, DGA, which provides the definition of "re-use" of data, specifying that "'re-use' means the use by natural or legal persons of data held by public sector bodies, for *commercial or non-commercial purposes* other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks".

As in some sectors of the legal system personal and non-personal data enjoy special protection, the Data Governance Act aims at favouring the re-use of these data too, where possible, without undermining the protection guarantees provided for by the special rules governing these areas.

In this respect Recital No. 6 can be useful, specifically where it specifies that "(…) Directive (EU) 2019/1024 and sector-specific Union law ensure that the public sector bodies make more of the data they produce easily available for use and re-use. However, certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data, in public databases are often not made available, not even for research or innovative activities in the public interest, despite such availability being possible in accordance with the applicable Union law, in particular Regulation (EU) 2016/679 and Directives 2002/58/EC and (EU) 2016/680. Due to the sensitivity of such data, certain technical and legal procedural requirements must be met before they are made available, not least in order to ensure the respect of rights others have over such data or to limit the negative impact on fundamental rights, the principle of non-discrimination and data protection. The fulfilment of such requirements is usually time- and knowledge-intensive. This has led to the insufficient use of such data. While some Member States are establishing structures, processes or legislation to facilitate that type of re-use, this is not the case across the Union. In order to facilitate the use of data for European research and innovation by private and public entities, clear conditions for access to and use of such data are needed across the Union."

Therefore, the Data Governance Act attempts to introduce legal solutions to make such data, ruled under a restrictive regime, available for a re-use for commercial and non-commercial purposes, preserving at the same time the respect for fundamental rights.

The role of public administration, in this respect, is extremely interesting, because it winds up acting, in the public interest, as an intermediary, in the logics of re-use of data which it holds for its institutional purposes, while preserving the protection of the subjects to whom these data refer to who, thanks to the action of public administration, can enjoy an enhanced system that protects their rights.[22]

While however in the field of the provision of "data intermediation services" referred to in Chapter III and data altruism referred to in Chapter IV the public sector bodies can contribute with those of the private sector to performing an intermediary role aimed at favouring data circulation, in the case of "Re-use" referred to in Chapter II intermediation can occur only through the action of the bodies acting in the public sector, regarding data, falling under certain categories, which they hold to pursue their institutional purposes. The subjects that operate in the private sector can interact with public administration and have access to said data and their re-use, for commercial and non-commercial purposes, within the limits and conditions of the specific legal regulations outlined therein (Articles 3-9 DGA)

3. *Data Governance Act and the re-use of (certain categories of protected) data held by public sector bodies, for commercial and non-commercial purposes*

The issue of the re-use of data held by public sector bodies is of course nothing new: specific regulations were already present in Directive 2019/1024/EU on open data and the re-use of public sector information.[23] For some categories of data, however, the movement follows more restrictive rules, owing to the need to protect trade and professional secrets, statistical confidentiality, intellectual property rights of third parties and fundamental rights connected to personal data.

[22] The mechanism can be partly compared to the services of data cooperatives, within the field of the provision of data intermediation services in the private sector, referred to in Recital No. 31, under Art. 2, para. 1, No. 15 and Articles 10-15 of the Data Governance Act. See F. Bravo, *Le cooperative di dati*, 757-799.

[23] J. Valero Torrijos, *Datos abiertos y reutilización en el contexto de la Estrategia europea de datos*, in *Tábula*, 2021, 201-213; T. Douville, *Open data des décisions de justice, cinq ans après : état des lieux et perspective*, in *Légipresse*, Vol. 65, No. HS1, 2021, 49-61.

Following the new European strategy on data governance, with the Data Governance Act the European legislator chose to favour the re-use of said data in this very field, creating at the same time the prerequisites to preserve a high level of protection to defend the requirements that the sectorial legislation, in the afore-mentioned fields, aimed to safeguard.

Art. 3, para. 1, DGA, therefore identifies the scope of application of the new regulatory provisions on re-use, which apply to "data held by public sector bodies which are protected on grounds of: (a) commercial confidentiality, including business, professional and company secrets; (b) statistical confidentiality; (c) the protection of intellectual property rights of third parties; or (d) the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024."[24]

The Data Governance Act therefore aims at enhancing the regulations related to the re-use of data held by public sector bodies, already provided for by Directive 2019/1024/EU on open data and the re-use of public sector information, by also applying it to other data, held by public sector bodies, who are under a restrictive data flow regime.

The goal is to build a trustworthy environment to increase the availability of personal and non-personal data for "secondary use" and, therefore, facilitate the re-use of data and the creation of innovative services and products based on data.

It can be considered a major component of the European strategy for data, which aims to bolster both the data economy and the data-driven society.

The introduction of regulations on the re-use of personal and non-personal data held by public administration provides a major role to public administration, which thus becomes a facilitator in the data movement and enhancement processes which it already has at its disposal by virtue of its institutional purposes.

It should be noted, however, that with the Data Governance Act the EU did not seek to require the public administration to make available the data it already holds for re-use: the Member States will decide to what extent public administration will be involved in the national law, with the risk of heterogeneous situations arising from this in the various national legal systems. In particular, Recital No. 11 DGA specifies that, in this respect, "This Regulation should not create an obligation to allow the re-use of data held by public sector bodies. In particular, each Member State should therefore be able to decide whether data is made accessible for re-use, also in terms of the purposes and scope of such access (…)." Moreover, the same Recital also adds that "This Regulation should complement and be without prejudice to more specific obligations on public sector bodies to allow re-use of data laid down in sector-specific Union or national law. Public access to official documents may be considered to be in the public interest. Taking into account the role of public access to official documents and transparency in a democratic society, this Regulation should also be without prejudice to Union or national law on granting access to and disclosing official documents. Access to official documents may in particular be granted in accordance with national law without imposing specific conditions or by imposing specific conditions that are not provided by this Regulation."

Of course, the role of public administration, in making available data and information that can have a strategic importance on the market, must be impartial. Otherwise it would dangerously alter the competition dynamics that the Data Governance Act sought to favour.

Thus, Art. 4 DGA forbids exclusive arrangements that give an advantage to some subjects to the detriment of others, unless the granting of the exclusive rights to the re-use of data constitutes a necessary measure to ensure the provision of a service or product of general interest that would otherwise be impossible to provide. In this case, however, the exclusive rights, which must be agreed on through an administrative act or a contract, are limited in time and are subject to the principle of transparency: they can only last up to twelve

[24] Art. 3, para. 2, DGA, however, clarifies that the provisions concerning the re-use of data foreseen in the Data Governance Act do not apply to the following further data categories: "(a) data held by public undertakings; (b) data held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit; (c) data held by cultural establishments and educational establishments; (d) data held by public sector bodies which are protected for reasons of public security, defence or national security; or (e) data the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State concerned, or, in the absence of such rules, as defined in accordance with common administrative practice in that Member State, provided that the scope of the public tasks is transparent and subject to review."

months and the reasons that made the exclusive rights necessary must be made public online, in a form that complies with the European regulations on the matter of public procurement.[25]

One of the key features of the regulations on the re-use of data covered in the DGA are the terms of the re-use provided by Art. 5.

Firstly, para. 1 determines that "Public sector bodies which are competent under national law to grant or refuse access for the re-use of one or more of the categories of data referred to in Article 3(1) shall make publicly available the conditions for allowing such re-use and the procedure to request the re-use via the single information point referred to in Article 8. Where they grant or refuse access for re-use, they may be assisted by the competent bodies referred to in Article 7(1).

Member States shall ensure that public sector bodies are equipped with the necessary resources to comply with this Article."

The European legislator, with the DGA, could have set the requirement for public sector bodies to make available the data for the re-use, but instead chose to have the Member States work on the more specific regulation. The national law will therefore regulate whether public sector bodies have the right to grant or reject the requests to access the data they themselves hold. The European regulation does not formally introduce an *obligation* of the public sector bodies of providing the data for re-use, but it does not prohibit this obligation from being introduced in the national law. In other words, the national legal systems will introduce criteria, principles, *obligations* and *rights*, by virtue of which the public sector bodies will make available the data to be devoted to re-use, which will consequently lead to a heterogenous situation across Member States, a far cry from the goal of achieving the homogeneity in EU law that a regulation, unlike a directive, is supposed to achieve. This is certainly a critical aspect, which suggests that there will be further regulatory measures implemented by the European legislator to create uniformity between national legal systems, at a later, riper stage.

The discretion of Member States is not boundless, given that, albeit with the criteria that will be set at a national level, they are nevertheless required to allow for the re-use of data belonging to the above-mentioned categories and to provide the public sector bodies with the necessary *resources* to achieve said goal. The discretion of Member States is also limited by the need to meet a set of principles generally applicable to public administrations, which however in Art. 5, para. 3, DGA are further specified with a particular focus on the re-use of data: "Conditions for re-use shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed. Those conditions shall not be used to restrict competition."

Apart from the impartiality principle, also in relation to the effects on the competition dynamics, transparency and proportionality, there is also a clear doctrine of necessity, which requires the conditions of re-use to be "objectively justified", not only meaning that they must guarantee a balanced reconciliation of the relevant interests, but also in the sense that they must lead to the achievement of the goal sought by the legislator (re-use of certain categories of protected data held by public sector bodies") with the smallest sacrifice possible of the opposed interest protected by the legal system (protection of the data subject, protection of the intellectual property rights, and so on), without this interest being devalued, undermined or destroyed in its funda-

[25] See Art. 4 (*Prohibition of exclusive arrangements*): "1. Agreements or other practices pertaining to the re-use of data held by public sector bodies containing categories of data referred to in Article 3(1) which grant exclusive rights or which have as their objective or effect to grant such exclusive rights or to restrict the availability of data for re-use by entities other than the parties to such agreements or other practices shall be prohibited.
2. By way of derogation from paragraph 1, an exclusive right to re-use data referred to in that paragraph may be granted to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible.
3. An exclusive right as referred to in paragraph 2 shall be granted through an administrative act or contractual arrangement in accordance with applicable Union or national law and in compliance with the principles of transparency, equal treatment and non-discrimination.
4. The duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded, the duration of the contract shall be the same as the duration of the exclusive right.
5. The grant of an exclusive right pursuant to paragraphs 2, 3 and 4, including the reasons as to why it is necessary to grant such a right, shall be transparent and be made publicly available online, in a form that complies with relevant Union law on public procurement.
6. Agreements or other practices falling within the scope of the prohibition referred to in paragraph 1 which do not meet the conditions laid down in paragraphs 2 and 3 and which were concluded before 23 June 2022 shall be terminated at the end of the applicable contract and in any event by 24 December 2024."

mental characteristics.
Within this framework, the DGA does not refrain from setting specific conditions for the re-use of data, which emphasise the new role given to public sector bodies within this context: not only of "intermediary" (in a broad sense) in the re-use of the data held by them, which in particular fall under the categories subject to specific protection, but also of active supervisor, facilitator and, above all, "*protector*" and "*enhancer*" of the rights of those who can be damaged by the movement of the data, belonging to specific protected categories, held by public sector bodies.
The latter, upon granting access to the data for re-use, are required to play an *active role*, which goes far beyond making available the data they already hold by virtue of the performance of institutional tasks. They must, in accordance with European and national law, do all that is necessary to "ensure that the protected nature of data is preserved (…)".[26]
The DGA, in particular, requires public sector bodies to "to grant access for the re-use of data only where the public sector body or the competent body, following the request for re-use, has ensured that data has been:
(i) anonymised, in the case of personal data; and
(ii) modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights (…)".[27]
This is a first active measure on data and in terms of control, both with the goal of tackling the risks of infringement of rights otherwise undermined by the movement of the data themselves within the framework of re-use strategies, and to ensure that said rights are preserved and not undermined.
The European legislator has envisaged a second important measure to the same end, by requiring that the access and re-use of said data – anonymised, modified, aggregated or treated, as specified above – occur "remotely within a *secure processing environment* that is provided or controlled by the public sector body"[28] or "within the physical premises in which the *secure processing environment* is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties."[29] Thus, in a general way in the field of re-use of data held by public sector bodies a solution that has already been tested at a European level for research on statistical microdata in the basis of Commission Regulation (EU) No. 557/2013 is applied.[30]
Moreover, a third measure required from public sector bodies entails the preservation of the integrity of the systems used to create a treatment environment that is safe for accessing and re-using data, with powers-duties of public administration both in terms of regulations and of control, that extend even to the results of the processing activity carried out by the data re-user, whose use may also be prohibited following the above-mentioned control.[31]
The guarantee and control functions performed by public service bodies when it comes to the re-use of data, together with that of "enhancer" of rights emerge from the further role assigned to them in the stage of information flow: they "(…) shall make the re-use of data (…) conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties that the re-user may have acquired despite the safeguards put in place"[32]; moreover, the public bodies who perform the re-use of data will receive any notification on the violations of data that may occur among data re-users, who are required to meet certain requirements.[33] For example the GDPR re-

[26] Art. 5, para. 3, DGA.
[27] Art. 5, para. 3, lett. *a),* DGA.
[28] Art. 5, para. 3, lett. *b),* DGA.
[29] Art. 5, para. 3, lett. *c),* DGA.
[30] See Commission Regulation (EU) No. 557/2013 of 17 June 2013 implementing Regulation (EC) No. 223/2009 of the European Parliament of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No. 831/2002.
[31] See Art. 5, para. 4, DGA: "In the case of re-use allowed in accordance with paragraph 3, points (b) and (c), the public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used. The public sector body shall reserve the right to verify the process, the means and any results of processing of data undertaken by the re-user to preserve the integrity of the protection of the data and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user."
[32] Art. 5, para. 5, DGA.
[33] In accordance with Art. 5, para. 5, DGA it is also set out that "(…) Re-users shall be prohibited from re-identifying any data subject to whom the data relates and shall take technical and operational measures to prevent re-identification and to notify any data breach resulting in the re-identification of the data subjects

quires that the data breach notification by performed by the data controllers to the relevant Data protection Supervisory Authority: this element highlights the special guarantee and control position of the public sector bodies.

The DGA also covers the possibility of the re-use of personal data not being done anonymously, for example if the anonymisation jeoparidises the utility of the data for the user.[34] Under these circumstances the data transfer operations by the public sector body, which holds the personal data, to the subject intending to use the data within the framework of the re-use strategies, may be performed only if there is a legal basis that allows this transfer of data even without the consent of the data subject[35] or if there is a specific consent coming from the data subjects.[36] Here too one can witness the proactive role of the public sector bodies which, based on the DGA's regulations, "shall make best efforts, in accordance with Union and national law, to provide assistance to potential re-users in seeking *consent* of the data subjects or *permission* from the data holders whose rights and interests may be affected by such re-use, where it is feasible without a disproportionate burden on the public sector body (…)".[37]

A similar regime is also applied to (non-personal) data deemed confidential at a commercial or statistical level, before which "(…) the public sector bodies shall ensure that the confidential data is not disclosed as a result of allowing re-use, unless such re-use is allowed in accordance with paragraph 6"[38] (abovementioned), on the basis of the data subjects' consent or the data holders' permission.

Regarding third categories of protected data held by public sector bodies, the DGA merely requires, categorically, that the "re-use of data shall be allowed only in compliance with intellectual property rights (…)"[39]: this requires the authorisation of the holder of intellectual property rights, unless the re-use falls under the scenarios of "fair use" provided for by the sectorial legislation.

There is however the risk that the regulations on the matter of intellectual property winds up hampering the European strategy on the re-use of data if it recognises the intellectual property rights directly in the hands of the public sector bodies. To avert this risk the DGA requires the latter not to exercise these rights in contrast with the purposes of the re-use of data: in particular it is set out that "(…) The right of the maker of a database as provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of data or to restrict reuse beyond the limits set by this Regulation."[40]

These are major provisions because they seek to prevent strategies by public administration aimed at not sharing data and even if the public sector bodies held intellectual property rights on the data, they "should, however, exercise their copyright in a way that facilitates

concerned to the public sector body. In the event of the unauthorised re-use of non-personal data, the re-user shall, without delay, where appropriate with the assistance of the public sector body, inform the legal persons whose rights and interests may be affected."

[34] Regarding the re-use of data, the approach of the European legislator, in the DGA, is to set a progressive safeguard, by adopting instruments of maximum protection, which can however by lightened progressively to avoid undermining the re-use strategy. Recital No. 15 DGA is particularly important in this respect, specifically in the part in which it states that "Before transmission, personal data should be anonymised, in order not to allow the identification of the data subjects, and data containing commercially confidential information should be modified in such a way that no confidential information is disclosed. Where the provision of anonymised or modified data would not respond to the needs of the re-user, subject to fulfilling any requirements to carry out a data protection impact assessment and consult the supervisory authority pursuant to Articles 35 and 36 of Regulation (EU) 2016/679 and where the risks to the rights and interests of data subjects have been found to be minimal, on-premise or remote re-use of the data within a secure processing environment could be allowed. This could be a suitable arrangement for the re-use of pseudonymised data (…)."

[35] For instance, when the processing is necessary: (i) "for compliance with a legal obligation to which the controller is subject" (Art. 6, para. 1, lett. *c*, GDPR); (ii) "in order to protect the vital interests of the data subject or of another natural person" (Art. 6, para. 1, lett. *d*, GDPR); (iii) "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Art. 6, para. 1, lett. *e*, GDPR); (iv) "for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" (Art. 6, para. 1, lett. *f*, GDPR); (v) "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy" (Art. 9, para. 2, lett. *i*, GDPR); and so on.

[36] See Art. 6, para. 1, lett. *a*, and Art. 9, para. 2, lett. *a*, GDPR.

[37] Art. 5, para. 6, DGA.

[38] Art. 5, para. 8, DGA.

[39] Art. 5, para. 7, DGA.

[40] Art. 5, para. 7, DGA.

re-use".[41]
Specific guarantees are then envisaged in the event that the re-user intends to transfer the data to a third country. In the case of personal data, the special regulations in the GDPR would be applied. In the case of non-personal data, on the other hand, the DGA introduces the requirement, of the re-user, to inform the public body on the intention of the re-user and of the purpose of the transfer, upon requesting the re-use, for the public body to exert further control functions, even to prevent the transfer until "the legal person whose right and interests may be affected of that intention (…) gives permission for the transfer."[42] In the meantime, the re-user must contractually undertake not only to meet, also in the event of transfer of data to a third country, the obligations covered by Art. 5, paragraphs 7 and 8, DGA on the flow across the EU of the data falling under the regulations of confidential information and intellectual property rights, but also to accept "the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body with regard to any dispute related to compliance with paragraphs 7 and 8."[43] To favour said contractual commitments, similarly to what is already provided for by the GDPR on the transfer of personal data to third countries, the European Commission may introduce, through its implementing acts, specific model contractual clauses to meet the above-mentioned requirements. In the event of a violation of the requirements envisaged for the transfer of data to a third country, the natural or legal person to which the right to re-use non-personal data was granted cannot perform the transfer to said third country.[44]
The push for personal and non-personal data flow is clear. To eliminate the uncertainties on the outcome of the re-use requests, they must be processed within two months since their reception, both in the event of an approval and of a rejection, unless different and shorter deadlines are set in accordance with national law: longer deadlines are not allowed.[45] The only exception provided by the DGA concerns the case of "exceptionally extensive and complex" re-use requests: here the two-month deadline can be prolonged for a maximum of thirty additional days, notifying "the applicant as soon as possible that more time is needed for conducting the procedure, together with the reasons for the delay."[46]
The complexity of the role played by public sector bodies on the re-use of data held by them is clear, so much so that the European legislator had to move in three further directions, so as to put into practice the new European strategy on data governance and make it more effective.
On the one hand there has been the introduction of the possibility, by the public bodies that allow the re-use of data belonging to the specific categories considered by the DGA, to impose fees, which "shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition."[47]
The non-discrimination principle does not prevent however different fees from being applied, in relation to specific needs, for example to incentivise the re-use of data for non-commercial purposes (as could be the case in the field of scientific research) or the re-use in favour of SMEs and start-ups subject to rules on State aid, or the re-use of data whose request comes from civil society or educational institutions. One may therefore apply reduced fees or reuse data free of charge. These would nevertheless be exceptions compared to the general principle, which envisages the application of a fee system, also for the service to be economically sustainable and efficient, by taking into account both the active role played by public bodies in this specific field (which is added to the normal institutional role they play) and of the costs related to the procedure carried out to meet the re-use requests.[48]
The fee system shall however be established at a national level by the single Member States, also regarding the criteria and methodology to calculate the fees and shall contrib-

[41] Recital No. 17, DGA.
[42] Art. 5, para. 9, DGA.
[43] Art. 5, para. 10, DGA.
[44] Art. 5, para. 14, DGA.
[45] Art. 9, para. 1, DGA.
[46] Art. 9, para. 1, DGA.
[47] Art. 6, para. 2, DGA.
[48] One must note that under Art. 6, para. 5, DGA it is specified that "Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of the categories of data referred to in Article 3(1) and limited to the necessary costs in relation to: (a) the reproduction, provision and dissemination of data; (b) the clearance of rights; (c) anonymisation or other forms of preparation of personal data and commercially confidential data as provided for in Article 5(3); (d) the maintenance of the secure processing environment; (e) the acquisition of the right to allow re-use in accordance with this Chapter by third parties outside the public sector; and (f) assisting re-users in seeking consent from data subjects and permission from data holders whose rights and interests may be affected by such re-use."

ute, once again, to the spread of heterogeneous choices across the EU.[49] At any rate, each public body is required to meet transparency principles, which in this case is the obligation to "publish a description of the main categories of costs and the rules used for the allocation of costs."[50]

On the other hand the public sector bodies, upon granting or rejecting the re-use of the data belonging to the specific categories covered by the DGA, must be assisted by one or more "competent bodies"[51] equipped with the necessary knowledge and means,[52] designed by each Member State, with the following tasks: (i) "providing technical support by making available a secur processing environment for providing access for the reuse of data";[53] (ii) "providing guidance and technical support on how to best structure and store data to make that data easily accessible";[54] (iii) "providing technical support for pseudonymisation and ensuring data processing in a manner that effectively preserves the privacy, confidentiality, integrity and accessibility of the information contained in the data for which re-use is allowed, including techniques for the anonymisation, generalisation, suppression and randomisation of personal data or other state-of-the-art privacy-preserving methods, and the deletion of commercially confidential information, including trade secrets or content protected by intellectual property rights";[55] (iv) "assisting the public sector bodies, where relevant, to provide support to re-users in requesting consent for re-use from data subjects or permission from data holders in line with their specific decisions, including on the jurisdiction in which the data processing is intended to take place and assisting the public sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible";[56] (v) "providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 5(10)", [57] in the event of transfers of non-personal data to third countries.

The Member States may assign a key role to the "competent bodies", by enabling them to grant themselves access for the re-use of the data belonging to the categories covered by the DGA, pursuant to European or national law which provides for such access to be granted. In said case all the provisions applicable to the public sector bodies that grant the re-use of data in accordance with the DGA shall be applicable to the "competent bodies", including the provisions on the matter of "Prohibition of exclusive arrangements" (Art. 4), "Conditions for re-use" (Art. 5), "Fees" (Art. 6) and "Procedure for requests for re-use" (Art. 9).

Finally, as a third measure, it has been decided that there will be the establishment by the Member States of "Single information points" with multiple tasks, aimed at making it easier to find the information on the re-use of data and the processing of the requests, with functions that "may be automated provided that the public sector body ensures adequate support."[58]

In particular the Single information points must: (i) make available and easily accessible all the information related to the conditions of re-use of data and the applicable fees;[59] (ii) "transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies (…), where relevant";[60] (iii) "make available by electronic means a searchable asset list containing an overview of all available data resources including, where relevant, those data resources that are available at sectoral, regional or local information points, with relevant information describing the available data,

[49] Art. 6, para. 6, DGA.
[50] Art. 6, para. 6, DGA.
[51] The "competent bodies" established from scratch by the Member States, or the latter may rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions laid down in the DGA. See Art. 7, para 1, DGA.
[52] In accordance with Art. 7, para. 3, DGA, "The competent bodies shall have adequate legal, financial, technical and human resources to carry out the tasks assigned to them, including the necessary technical knowledge to be able to comply with relevant Union or national law concerning the access regimes for the categories of data referred to in Article 3(1)."
[53] Art. 7, para. 4, lett. *a*, DGA.
[54] Art. 7, para. 4, lett. *b*, DGA.
[55] Art. 7, para. 4, lett. *c*, DGA.
[56] Art. 7, para. 4, lett. *d*, DGA.
[57] Art. 7, para. 4, lett. *e*, DGA.
[58] Art. 8, para. 1, DGA. The path towards using automated systems has been inaugurated here too, including those based on AI (Artificial Intelligence), which nevertheless require human oversight, as can be witnessed in Recital No. 26, in which it is noted that "Sufficient human oversight should be ensured in the transmission process." See also G. Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Milan, Wolters Kluwer-Cedam, 2023.
[59] Art. 8, para. 1, DGA.
[60] Art. 8, para. 3, DGA.

including at least the data format and size and the conditions for their re-use."[61]
Furthermore, the single information points can "establish a separate, simplified and well-documented information channel for SMEs and start-ups, addressing their needs and capabilities in requesting the re-use of the categories of data referred to in Article 3(1)."[62]
To make the action of the single information points more effective, the decision made was to develop them at various territorial levels. A single information point is established at national level, by each Member State, which may designate, to this end, a new body or an existing body or structure.[63] Along with the "national" single information point, each Member State can then envisage other "sectoral, regional or local information points", connected to the central one, located at a national level. The national single information points, in turn, are connected to a European single access point, established by the European Commission, "offering a searchable electronic register of data available in the national single information points and further information on how to request data via those national single information points."[64]

4. ***Critical aspects***

The critical aspects of the new regulations on the re-use of data by the public sector bodies are certainly numerous and some of them have already been highlighted.
The European legislator chose to use a regulatory source that ultimately leads to an overall uniformity in the Member States' legislation, by resorting to the European "regulation" to regulate European data governance, but, at least regarding the re-use of data, the European legislator wound up delegating many of the identified solutions to the discretional choices of the Member States, thus undermining the goal of regulatory uniformity within the EU: take for example the choice of letting the Member States determine whether the Public sector bodies have the right to decide whether to grant or reject access for the re-use of one or multiple categories of data, as well as determine the applicable fees for the re-use, in accordance with Articles 5 and 6 DGA.
Moreover, apart from the lack of uniformity at European level, the need for regulatory measures at a national level leads to an unavoidable postponement of the regulations' implementation, as one must wait for regulatory acts in the national legal systems, which result in a delayed actual implementation of the regulations in question compared to the deadline envisaged by Art. 38 DGA, in accordance with which the regulation "shall apply from 24 September 2023."
Some critical aspects had been highlighted by the EDPB and the EDPS in the Joint-Opinion No. 3/2021 on the Proposal for a regulation of the European Parliament and of the Council on Euopean data governance (Data Governance Act), v. 1.1, 9 June 2021. These are, however, findings that are not universally deemed valid.
The first of these concerns the ambiguity and uncertainty between the application boundaries of the regulations on the re-use of data in the DGA and the regulations provided for by Directive (EU) 2019/1024 on the matter of open data,[65] which should have been better specified, not only within the Recitals, but also with dedicated articles of the regulation.[66]
In the final text of the DGA, Art. 3, para. 1, lett. d), clarifies that Chapter II, on the "Re-use of certain categories of protected data held by public sector bodies", "(…) applies to data held by public sector bodies which are protected on grounds of: (…) d) the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024."
Art. 1 of said Directive sets out that "In order to promote the use of open data and stimulate innovation in products and services, this Directive establishes a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of (…) existing documents held by public sector bodies of the Member States (…)" and that, however, it "(...) does not apply to (…) documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the

[61] Art. 8, para. 3, DGA.
[62] Art. 8, para. 3, DGA.
[63] Art. 8, para. 4, DGA.
[64] Art. 8, para. 4, DGA.
[65] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.
[66] See EDPB-EDPS, *Joint Opinion No. 3/2021*, Section 3.3.1.

protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data."[67]

The regulations on the matter of "open data and re-use of public sector information", therefore, do not exclude beforehand the possibility of the re-use of personal data held by public sector bodies: it allows it when it does not violate the regulations on the matter of personal data protection, including the cases in which one resorts to the anonymisation of personal data. In fact, Recital No. 52 of the Open Data Directive expressly states that "This Directive does not affect the protection of individuals with regard to the processing of personal data under Union and national law, particularly Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council and including any supplementing provisions of national law. This means, inter alia, that the re-use of personal data is permissible only if the principle of purpose limitation as set out in point (b) of Article 5(1) and Article 6 of Regulation (EU) 2016/679 is met. Anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. Rendering information anonymous is a means of reconciling the interests in making public sector information as re-usable as possible with the obligations under data protection law, but it comes at a cost. It is appropriate to consider that cost to be one of the cost items to be considered to be part of the marginal cost of dissemination as referred to in this Directive."

By taking this into account, however, the new Data Governance Act encourages the application of the regulations on the re-use of data held by public sector bodies contained in the open data directive,[68] while also proposing to extend the scope of data re-usability, if this is not possible in accordance with the regulations contained in the above-mentioned directive. Recital No. 10, DGA, is very clear about this, where it is clarified that "The categories of data held by public sector bodies which should be subject to re-use under this Regulation fall outside the scope of Directive (EU) 2019/1024 that excludes data which is not accessible due to commercial and statistical confidentiality and data that is included in works or other subject matter over which third parties have intellectual property rights. Commercially confidential data includes data protected by trade secrets, protected know-how and any other information the undue disclosure of which would have an impact on the market position or financial health of the undertaking. This Regulation should apply to personal data that fall outside the scope of Directive (EU) 2019/1024 insofar as the access regime excludes or restricts access to such data for reasons of data protection, privacy and the integrity of the individual, in particular in accordance with data protection rules (…)."[69]

Therefore the interpreter, during the implementation, shall determine when the regulations on the re-use of data referred to in Directive (EU) 2019/1024 are applicable and when the regulations referred to in the DGA are. There may be cases of partial overlapping, which should be resolved with the application of the DGA, both because it came after the 2019 Directive (*lex posterior derogat priori*), and because it must be considered a special law compared to the more general law contained in the directive *(lex speciali derogat generali)*. It must be noted, in this respect, that in the DGA the regulations of Chapter II are more limited both from a subjective point of view, in that it only concerns data held by *public sector bodies*, with the exclusion of data held by public undertakings, (included instead in the 2019 Directive), and from an objective point of view, in that it only concerns "*certain categories of protected data*" (while the regulations on the re-use contained in the 2019 Directive covers larger categories of data).

Moreover, the regulations contained in the DGA are immediately applicable in all Member States and would prevail over the rules of the national legislation of the Member States,

[67] Art. 1, para. 2, lett. h, Directive (UE) 2019/2014.

[68] See Recital No. 9, DGA: "(9) In order to facilitate the protection of personal data and confidential data and to speed up the process of making such data available for re-use under this Regulation, Member States should encourage public sector bodies to create and make available data in accordance with the principle of 'open by design and by default' referred to in Article 5(2) of Directive (EU) 2019/1024 and to promote the creation and the procurement of data in formats and structures that facilitate anonymisation in that regard."

[69] See Recital No. 10, DGA, which also adds that "(…) The re-use of data, which may contain trade secrets, should take place without prejudice to Directive (EU) 2016/943, which sets out the framework for the lawful acquisition, use or disclosure of trade secrets."

rendered in implementation of the previous directive, even more so if one considers the fact that the DGA lacks the rules aimed at establishing that Directive 2019/1024 would prevail in the event of contrast with the Regulation, [70] unlike what is provided for in other regulatory fields, including those regulating the protection of personal data and competition law.[71]

A second finding by the EDPB and the EDPS concerns the heterogeneity of the categories of data covered by the regulations on re-use outlined in the DGA, which winds up generating applicational uncertainties: in particular when it brings together under a single "umbrella" the heterogeneous categories of personal and non-personal data (regarding intellectual property rights and confidential information protected for commercial or statistical reasons) and suggests that the regulations on the matter of personal data protection hinders the re-use of data, thereby slowing down the general interest and the economy.[72] The EDPB and the EDPS even describe these aspects as "*regrettable*, since it suggests the idea of data protection regulation as impeding the free movement of personal data, rather than laying down the rules of free flow of personal data while protecting the rights and interests of the persons concerned."[73]

Based on the regulatory framework of the DGA, analysed above, I believe that this judgment is far too harsh and not in line with the approach adopted by the European legislator who, by further incentivising the re-use of certain categories of data held by public sector bodies, has implemented a system that is particularly focused on realising the protection of the rights and freedoms of data subjects and making it effective, also thanks to the new role outlined for public administration and the further adjustments (i.e. secure processing environment; competent bodies).[74]

Other issues emerge regarding the coordination between the DGA and the GDPR.

What is certainly unfortunate is the introduction of subjective categories, such as those of data holder and data user, which are not well coordinated with those used in the GDPR (data controller, data processor, data subject) and can potentially create great uncertainty in the implementation of the regulations on the matter of European data governance.[75] The uncertainty is then exacerbated by the translation choices made in the national legal systems, such as in Italy, where data processor is translated as "titolare del trattamento" and data holder as "titolare dei dati". The interpreter of the regulation once again will be tasked with creating a system of these subjective categories in European and national law, while taking into account the interactions between the regulations on the matter of data protection and those on the matter of data governance.

Then it must be noted that, in general, the DGA does not introduce new legal bases for the lawfulness of processing, therefore the personal data processing performed upon the re-use are only legitimate if the legal basis envisaged by Articles 6-9 of the GDPR are met. In this respect the final text of the DGA, compared to the text of the proposal, is clearer, as is shown by Art. 5, para. 6, DGA and, above all, by Art. 1, para. 3, DGA, where it is expressly specified that "(…) This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations

[70] An implicit reference to the rules of Directive (EU) 2019/1024 can be found in Art. 2 DGA, but its formulation does not allow for the former to prevail on the latter in every situation: on the contrary, the formulation seems to indicate that the rules of the DGA and the further provisions of European and national law are applicable, provided that they guarantee (and do not limit) the re-use and access to data. The above-mentioned Art. 2 DGA in fact clarifies that "(…) This Regulation is without prejudice to: (a) specific provisions in Union or national law regarding the access to or re-use of certain categories of data, in particular with regard to *the granting of access* to and *disclosure* of official documents; (b) the obligations of public sector bodies under Union or national law to *allow* the re-use of data or to requirements related to processing of non-personal data."

[71] In fact, Art. 1, para 3 and 4, DGA sets out that "Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation. In particular, this Regulation is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, including with regard to the powers and competences of supervisory authorities. In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data shall prevail. This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations (EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680" (para 3) and that "This Regulation is without prejudice to the application of competition law" (para 4).

[72] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para. 66-67.

[73] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para. 68.

[74] See above, in this work, Section No. 3.

[75] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para. 29-46.

(EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680."

It must however be noted that the DGA, upon outlining the conditions of re-use of personal data, legitimises it [the re-use] when the data are anonymised by the public sector body holding them. However, the anonymisation process too, mentioned in the DGA, is a processing operation that would require the presence of a legal basis in accordance with the GDPR. It is not certain that the anonymisation is a processing operation covered by the legal basis used to legitimise the original processing activity, while in the DGA it is peacefully covered as a systematic operation, a default operation, to guarantee the flow of data in the perspective of re-use. In this case the DGA seems to introduce a new element compared to the GDPR, as it envisages at a regulatory level an anonymisation obligation, which can easily be traced back to the legal categories of the GDPR. It would therefore be a processing operation whose legal basis was a regulatory requirement in accordance with Art. 6, para. 1, lett. *c*), GDPR,[76] or in the (substantial) public interest pursued by the public sector body to achieve, in accordance with the rights of the data subjects, the re-use purposes of the data sought by the European legislator and the anonymisation operation is therefore based on Art. 6, para. 1, lett. *e*),[77] and Art. 9, para. 2, lett. *g*), GDPR,[78] to connect to the regulatory provision contained in Art. 5, para. 3, lett. a(i), DGA, which requires the anonymisation of personal data the meet the requirements of re-use, while preserving the free flow of data without undermining the rights and freedoms of the data subjects.

From a different perspective, the EDPB and the EDPS highlight the need to nevertheless meet the principles of data protection described in Art. 5, paragraphs 1 and 2, GDPR,[79] including the principle of purpose limitation,[80] which limits the scenario of secondary use of personal data to the boundaries outlined by Art. 6, para. 4, GDPR, whereby "Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law (…), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

The solutions proposed by the DGA move in a "complementary" direction: the regulation of the re-use of certain particular categories of data held by public sector bodies does not affect the secondary use referred to in Art. 6, para. 4, GDPR – which is therefore implicitly confirmed – but rather the concrete and effective possibility of using personal data for further purposes other than those of initial data collection, both through anonymisation (and the envisaging of instruments to make it more concretely possible), and through collection mechanisms of a new consent of the data subjects – where anonymisation is not a viable option – to legitimise the further processing of personal data, for purposes not considered upon the initial collection.

Another issue arises for all the scenarios in

[76] Based on Art. 6, para 1, lett. c), GDPR, "Processing shall be lawful only if and to the extent that at least one of the following applies: (…) processing is necessary for compliance with a legal obligation to which the controller is subject (…)".

[77] According to Art. 6, para 1, lett. e), GDPR, "Processing shall be lawful only if and to the extent that at least one of the following applies: (…) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (…)".

[78] In accordance with Art. 9, para 2, let. e), GDPR, the prohibition of processing data belonging to specific categories of data shall not be applied in the event that "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

[79] For an analysis of the legal regulations of the "Principles" on the matter of personal data protection see F. Bravo (ed. by), *Dati personali. Protezione, libera circolazione,* governance. – Vol. 1, *Principi*, Pisa, Pacini, 2023.

[80] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 73-75.

which the personal data cannot be anonymised: the subsequent re-use may occur with the consent of the data subject which the public sector body will seek to obtain from the data subject, unless there is another legal basis for the processing of personal data other than consent. The critical aspect however derives from the need to meet both the principle of purpose limitation, which requires the purpose of the processing to be clearly and specifically identified and for the processing not going beyond this purpose,[81] and the principles of precision and granularity of consent which, to be valid, must be given based on a duly specific and limited illustration of the purposes of the processing operation that will be pursued.[82]

Providing general consent to the re-use of data is therefore not sufficient, as the purpose of the processing operation one intends to pursue must be clearly outlined, otherwise the consent would inevitably be null and void. Moreover, natural persons are often required to provide their data to public sector bodies based on the requirements of the law or upon the request of a public service and the absence of clear information regarding the re-use of data and the purposes pursued may violate the principles of transparency and fairness provided for by the GDPR.[83]

From a different perspective, one must also verify the validity of the consent when it comes to freedom: the regulations on the re-use of data in the DGA envisages that the public sector bodies must act to request the consent for the processing of personal data for re-use to the subjects towards whom they play an institutional role, therefore potentially resulting in a clear situation of power imbalance, which undermines the freedom of the consent provided by the data subjects.[84]

The specificity of the subject actually seems to indicate that the public sector bodies involved the citizens by allowing them to participate in a collaborative and open manner in the procedures aimed at allowing the re-use of their personal data.[85] This should also lead to restoring a certain order between public power, in the hands of the body that acts to request the consent for the processing of data for re-use, and the data subject called upon to give their consent, thus giving back validity to the consent, when it comes to the freedom requirement,[86] although it would be far better for the re-use scenarios to be determined directly based on a regulatory measure, either from the EU or national,[87] that is of an administrative

[81] In accordance with Art. 5, para 1, lett. b), GDPR, "Personal data shall be (…) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')".

[82] These elements come from the definition of consent, contained in Art. 2, para 1, No. 11, GDPR ("'consent' of the data subject means any freely given, *specific*, informed and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"). See also F. Bravo, *Le condizioni di liceità del trattamento*, in G. Finocchiaro (ed.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 110; D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, in *Giurisprudenza italiana*, 2019, 12, 2783-2789.

[83] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 84.

[84] In this respect it has been noted that "(…) it is unclear the role of the public sector body in supporting re-users in obtaining the consent for the reuse by the data subject. As a further remark on Article 5(6) of the Proposal, the EDPB and the EDPS point out that this provision establishes an obligation for public sector bodies ("shall support"), whose content is not well defined. More to the point, the legal basis under the GDPR for contacting data subjects to collect their consent for the re-use should be specified, as well as the respective responsibility related to obtaining a valid consent under Article 7 of the GDPR. In this regard, it should also be taken into account the clear imbalance of power which is often present in the relationship between the data subject and the public authorities. In this context, in line with the GDPR accountability principle, the EDPB and the EDPS recall that the choice of an appropriate legal basis for the processing of personal data, as well as the demonstration that the chosen legal basis (in this case consent) can be validly applied, lies on the data controller". See EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 82.

[85] The EDPB and EDPS recommended "to define in the Proposal [of the DGA] adequate means by which individuals may participate, in an open and collaborative manner, in the process of allowing the re-use of their personal data". See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 85.

[86] In this direction see EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 19 May 2021, 6: "(…) due to the fact that the consent of the data subject might not be considered freely given due to the imbalance of power which is often present in the relationship between the data subject and the public authorities, the Joint Opinion expresses concerns on Article 5(6) of the DGA, and, more broadly, invites the co-legislators to clearly define in the Proposal adequate models of 'civic participation', by which individuals may participate, in an open and collaborative manner, in the process of defining the scenarios allowing the re-use of their personal data, following a bottom-up approach to open data projects (…)."

[87] See, again, EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 6: "The Joint Opinion also recommends amending the

instrument of a general nature, if – as is the case of the Italian legal system – this is allowed by the national legislation.[88]

Another critical aspect concerns the matter of the re-use of personal data regarding above all "sensitive sectors" such as healthcare. According to the EDPB and the EDPS, the DGA was supposed to set, in these sectors, the necessary requirements of the protection of personal data, as well as the related conditions and specific data protection safeguards"[89] to meet for the re-use of data, including the data protection impact assessment (DPIA) pursuant to Art. 35 GDPR, also necessary to found the decision on re-use.[90] The choice of the European legislator, in the DGA, was however different: the obligation to perform the DPIA was already envisaged in the GDPR, and said European Regulation remains applicable to the cases of re-use of personal data held by public sector bodies, and prevails in the event of conflict with the provisions of the DGA. As it is already regulated in the GDPR, there is no need to envisage the DPIA obligation in a systematic way in the DGA too for all the scenarios of re-use of data: the applicational boundaries of this obligation shall nevertheless remain those outlined by the GDPR. The obligation to perform the DPIA, for the re-use of non-anonymised personal data, is in any case mentioned in the Recitals.[91]

A further critical aspect highlighted by the EDPB and the EDPS concerns the role of the competent bodies and the relationship with the role of the national Data Protection Supervisory Authorities envisaged in the GDPR and in Art. 8 of the Charter of Fundamental Rights of the EU (CFREU): the risk is that it may generate a multiplying effect of public subjects with competence in the field of data protection, to leave only to the oversight authorities that have already been established with the GDPR, and an interference between tasks and functions in said matter.[92] In this respect it has been specified, on the one hand, that it is by no means clear whether a Data Protection Supervisory Authority can be identified as a "competent body" under Art. 7 DGA;[93] on the

DGA to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or Member State law which lays down a list of clear compatible purposes for which the further processing may be lawfully authorised or constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR."

[88] E.g. Art. 2-b ("Legal basis to process personal data for the performance of a task carried out in the public interest or in the exercise of official authority"), para 1, of the Italian Personal Data Protection Code (D.Lgs. 196/2003), Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (As amended by decree-law No 139 of 8 October 2021 subsequently enacted and amended by way of Law No 205 of 3 December 2021). According to the Art. 2-b cited, "The legal basis mentioned in Article 6(3), letter b), of the Regulation shall be a law or a regulation or an *administrative instrument of a general nature*".

[89] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 87.

[90] The EDPB and EDPS highlighted that "according to the GDPR, the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommend to include in the text of the Proposal that a DPIA must be performed by public sector bodies in case of data processing falling under Article 35 of the GDPR. The DPIA will help to identify the risks and the appropriate data protection safeguards for the re-use addressing those risks, in particular for specific sector routinely with special categories of personal data (…)". See EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 88, where it is also specified that "(…) The decision on the re-use, in addition to being grounded on Union or Member State law, especially for some "sensitive sectors" (healh sector, but also transport or energy grid) should be based on this assessment, as well as the specific conditions for the re-users and the concrete safeguards for data subjects (for example, clarifying the risks of re-identification of anonymized data and the safeguards against those risks). Finally, the results of such assessment, whenever possible, should be made public, as a further measure enhancing trust and transparency".

[91] The obligation to carry out the DPIA pursuant to Article 35 GDPR is mentioned in Recital No. 15 of the DGA: "(…) Before transmission, personal data should be anonymised, in order not to allow the identification of the data subjects, and data containing commercially confidential information should be modified in such a way that no confidential information is disclosed. Where the provision of anonymised or modified data would not respond to the needs of the re-user, subject to fulfilling any requirements to carry out a *data protection impact assessment* and consult the supervisory authority pursuant to Articles 35 and 36 of Regulation (EU) 2016/679 and where the risks to the rights and interests of data subjects have been found to be minimal, on-premise or remote re-use of the data within a secure processing environment could be allowed (…)." See also Recital No. 7, DGA.

[92] EDPB-EDPS, *Joint Opinion No. 3/2021*, para 104-106.

[93] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 103, where, regarding the competent bodies referred to in Art. 7 DGA it was specified that "(…) despite those bodies are essentially tasked with support and advisory duties vis-à-vis public sector bodies for data re-use, some of their tasks deal with implementing the safeguards set out in the data protection legislation and fos-

other hand the use of "competent" in "competent bodies" under the above-mentioned Art. 7 was criticised;[94] finally, what was highlighted was the need to establish collaboration mechanisms between competent bodies and the Data Protection Supervisory Authorities, with the guiding role played by the latter, "to ensure a coherent application of these provisions."[95]

A final critical aspect to be considered concerns the fee system envisaged by Art. 6 DGA, which in the DGA would constitute the rule, while in the Open Data Directive it would be the exception before the general principle of gratuity of the re-use of data: this contradiction, however, highlighted once again by the EDPB and the EDPS, is actually just apparent.[96] Directive (EU) 2019/1024, in fact, under Art. 6 ("Principles governing charging") envisages, in para. 1, that "The re-use of documents [and data] shall be free of charge", but it also adds that "However, the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed."[97] Therefore, gratuity is a principle that can be applied only if the public sector bodies perform the re-use of data that are not under specific protection regimes: otherwise, if these bodies are required to protect personal data or commercially confidential information, the general rule is that it is allowed to apply fees for covering the costs taken on to guarantee the protection requirements. In the DGA the regulations on the re-use of data held by public sector bodies specifically concerns "certain categories of protected data", therefore the solution proposed in the DGA appears completely compliant with the choices also made in the Open Data Directive. The criticism of the EDPB and the EDPS seems to miss the mark.

A different matter is the incentive system. It has been highlighted that the regulations envisaged in the DGA seem "(…) to introduce financial incentives to public sector bodies to allow the re-use of personal data."[98] Moreover, in the same way it has also been noted that Art. 6 para. 4, DGA introduces a system of fee incentives to favour the re-use of data in the non-commercial sector or in the sector of State aid,[99] with possible repercussions on the validity of the consent to the processing of personal data with the purpose of re-use and on the actual exercise of the right to revoke one's consent.[100] Also in this case the concerns seem exaggerated, given that the incen-

tering the protection of the rights and interests of individuals with regards to their personal data. However, Chapter II (…) does not clarify whether data protection supervisory authorities – to which the GDPR also confers, among others, advisory powers – may be designed as the competent body under Article 7 (…)" of the DGA.

[94] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 105: "Furthermore, should specific bodies be designated to assist public sector bodies and data re-users and be entrusted to grant access for the reuse of data, including personal data, such bodies may not be referred as 'competent' as they would not act s a supervisory authority able to monitor and enforce the provisions related to the processing of personal data. In order to ensure legal certainty and consistency of the application of the EU acquis in the field of personal data protection, the activities and obligations of such designed bodies shall also be subject to the direct competence and supervision of data protection authorities, when personal data is involved."

[95] EDPB-EDPS, *Joint Opinion No. 3/2021*, para 106.

[96] For this criticism see, again, EDPB-EDPS, *Joint Opinion No. 3/2021*, para 96.

[97] Still in accordance with Art. 6 of the Directive (UE) 2019/1024, the principle of gratuity f re-use does not apply in the case of "public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks" e di "public undertakings", for which "the total charges shall be calculated in accordance with objective, transparent and verifiable criteria. Such criteria shall be laid down by Member States. The total income from supplying and allowing the re-use of documents over the appropriate accounting period shall not exceed the cost of their collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment, and — where applicable — the *anonymisation of personal data* and measures taken to protect commercially confidential information. Charges shall be calculated in accordance with the applicable accounting principles."

[98] EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 97.

[99] See EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 98, where it is specified that "It also has to be noted that Article 6(4) imposes an obligation to public sector bodies to "take measures to incentivize the reuse of the categories of data referred to in Article 3 (1) [which include personal data] for non-commercial purposes and by small and medium-sized enterprises in line with State aid rules."

[100] See, finally, EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para. 99, where, regarding the system of fee incentives it was noted that "This aspect (…) is problematic from a data protection viewpoint, under both legal and practical implementation's perspective. In particular, the lack of clarity on the type of incentives and addressees thereof may raise additional questions as to whether consent, as one of the legal basis relied upon under Article 5(6) of the Proposal for the re-use personal data, will be the appropriate legal ground, especially with regard to the individuals' freedom of choice to refuse to provide their consent to the re-use of their personal data or to withdraw it."

tives do not operate in favour of the data subjects, for the purposes of providing one's consent to the data processing, but rather towards the data users, who request access or the transfer of the personal data held by public sector bodies, after the consent of the data subjects has already been given. It seems as though the data subjects cannot receive any pressure from the data users, to which the fee incentives are applied, so much so that the interactions for the re-use are intermediated by the public sector bodies, called upon to exercise a guarantee function and to "enhance" the rights of the data subjects themselves.

5. ***New prospects***

The different approach introduced in the Data Governance Act (DGA), compared to the Open Data Directive (ODD), on the re-use of protected categories of data held by public administration, paves the way towards a new role of public sector bodies.

These bodies, apart from using the personal and non-personal data at their disposal for their functions, tied to the achievement of public interest, are called upon to act to ensure the flow of the data belonging to protected categories. They are asked to implement what is necessary to ensure both the fruition of the data for the data users, and an adequate level of protection of the rights and interests that the legal system chose to ensure by regulating certain categories of protected data considered in the DGA.

Within this context, public bodies seem to be called upon to reinterpret their action based on the principle of solidarity, by implementing the sovereign powers (as traditionally understood) and by establishing a new relationship with the citizens, whereby the latter see their ability to dialogue with public administration grow, as well as their areas of "active freedom", which come with greater duties and responsibilities for public administration.[101] The public sector bodies become not only intermediaries of the data they hold and facilitators of the free flow of data for commercial and non-commercial purposes not connected to the exercise of sovereign powers, but also subjects with a guarantee function towards those who, because of the nature of these data, have the right to hold a high level of protection of their rights and interests, connected to these data. The DGA outlines an enhanced protection, as it identifies specific protection measures, which translate into duties for public administration: to guarantee the re-use of data the DGA envisages that public administration must implement or oversee the anonymisation of public data, where possible, as well as the adoption of specific security measures, including the establishment of a secure processing environment. The guarantee and enhancement functions of the rights of the subjects to whom these categories of data refer to are then further enhanced with the action of the competent bodies, which are complemented with the action of the single information points, for the flow of data to be more impactful within a framework of re-use.

The relevant regulations overlook some important aspects, which will have to be addressed by the national legislators and by the relevant legal theory.

One concerns the profiles of responsibility that this new role entails for the public sector bodies and the competent bodies, for example where the anonymisation of data has not been carried out or verified correctly by public administration, or if the secure processing environment has not been correctly set up or managed or, also, if the public sector bodies, after receiving the notification of a violation of the non-personal data subject to protection (for example regarding trade secrets or intellectual property) did not act accordingly to counter the violation and curb the damage endured by those whose rights have been infringed.

Another important aspect, which must be examined, is how the re-use of the data held by public bodies will be contractualised, for commercial and non-commercial purposes. While when it comes to non-personal data one can resort to tried-and-tested concepts within the framework of intellectual property law, through the use of licenses, when it instead comes to personal data one must refrain from opting for easy and hasty solutions that are not compliant with European law. When it comes to personal data one cannot identify an ownership of the public sector bodies or other entities holding personal data,[102] nor can contracts

[101] See A.G. Orofino, *La solidarietà in diritto ammnistrativo: da strumento di protezione dell'individuo a parametro di disciplina del rapporto*, in *Il diritto dell'economia*, 2020, 2, 594; F. Benvenuti, *Il nuovo cittadino. Tra libertà garantita e libertà attiva*, Venice, Marsilio, 1994, *passim*.

[102] G. Alpa, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, Zorzi Galgano (ed.), Milan, Wolters Kluwer-Cedam, 2019, 11. See also V. Zeno Zencovich, *Do "data markets" ex-*

on the re-use of personal data have as their object the "sale" of data: when it comes to personal data that are not anonymised, one will have to take into account the specific aspects of the GDPR's regulations, as "one of [its] main purposes (…) is to provide data subjects with control over personal data relating to them",[103] preventing personal data from being deemed "a 'tradeable commodity'. An important consequence of this is that even the data subject can agree to the processing of his or her personal data, he or she cannot waive his or her fundamental rights. As a further consequence, the controller to whom consent has been provided by the data subject to the processing of her or his personal data is not entitled to 'exchange' or 'trade' personal data (as a so-called 'commodity') in a way that would result as not being in accordance with all applicable data protection principles and rules."[104]

This must not lead to the conclusion that personal data cannot be the object of contracts regulating their use, but rather that the adopted contractual solutions must be compliant with the specific nature of the fundamental right attributed to the data subject. Personal data can be the temporarily used for legitimate and specific purposes and in compliance with the principles indicated by the GDPR (including those of lawfulness, transparency and fairness, data minimisation, purpose limitation, storage limitation), which (also) have a limitative scope of contractual autonomy, to safeguard the rights and fundamental freedoms of the data subject.

Another very important aspect concerns civic participation. Where it is not possible to anonymise personal data, the public sector bodies are required to obtain the consent of the data subjects for the re-use of personal data, with the above-mentioned problems regarding the validity of the consent acquired by the public body holding the data, given the imbalance of power between public administrations (or at any rate public sector bodies) and the data subjects. The solution put forward by the EDPB and the EDPS, aimed at emphasising civic participation, is interesting for two reasons:

(i) on the one hand it operates on a legal level and aims at eliminating the imbalance present between public administration and the citizen-data subject, through collective measure mechanisms, based on civic participation models, which can also be implemented through associations of citizens and the data subjects. This paves the way toward new forms of protection and new ways to exercise one's rights,[105] in which the single individual, who is powerless before the power of the data controller, is called upon to join organisations that can more effectively protect their interests;[106]

(ii) on the other hand, the solution is particularly important at an ethical level, because it aims at more concretely implementing the FAIR principles (which were also already mentioned in the ODD as well as in the DGA)[107] and put in place ethical models of data re-use, also if they have commercial purposes, as well as non-commercial ones.

Thus a new data governance is emerging, with the new role of public administration: with the new regulations of the DGA, public administration is tasked with managing personal data not to exercise sovereign powers by supervising the citizens-data subjects, but – also in the governance of the territory (e.g. the Urban Digital Twins) – but both to ensure a greater and more effective flow of data, with an increase in collective, economic and social welfare, and to enhance the individual protection of natural and legal persons.

In other words, the regulations on re-use leverages data governance to maximise the enhancement of data, understood in its broadest sense.

ist?, 2019, 2, 25 ff., para. 3; A. Singh, *Protecting Personal Data as a Property Right*, in *ILI Law Rev.,* 2016, 123; P. Hugenholtz, *Data property: unwelcome guest in the house of IP*, in *Better Regulation for Copyright: Academics meet Policy Makers*, Reda, Brussels, 2017, 65-77.

[103] EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 4.

[104] EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 4.

[105] According to F. Benvenuti, *Il nuovo cittadino. Tra libertà garantita e libertà attiva*, *passim*, acknowledging the citizens' right to participation translates into making them a part of a relationship on an equal footing with the public system.

[106] This phenomenon is very reminiscent both of the forms of collective consumer protection, in European and national regulations on the matter of consumer protection (e.g. the role of consumer associations and collective actions) and of the new forms of protecting the interests of the data subjects through data cooperatives, which are also covered in the DGA.

[107] See Recital No. 2, DGA: data should be findable, accessible, interoperable and re-usable (the FAIR data principles). See also Recital No. 27 and Art. 10, ODD (Open Data and Public Sector Information Directive, Directive 2019/1024/UE).

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 35-42
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 04

*From Transparency and Reuse of Public-Sector Information to Data Spaces: The Evolution of EU Regulation**

Julián Valero Torrijos
(Full Professor of Administrative Law at the University of Murcia)

ABSTRACT The regulation of eGovernment and transparency of public bodies has mainly focused on a document-based management model. However, technological innovation demands a different approach based on data and the involvement of private entities. This paper analyses the most recent evolution of European regulation in this field, characterised by the central role of governance and data spaces.

1. *EU Regulation on Open Data and Reuse of Public-Sector Information as the Starting Point*

One of the main objections to the most widespread information management systems in the field of Public Administration from the perspective of technological innovation is the absence of an advanced approach when regulating access to information. Especially regarding the conditions under which it must take place to facilitate the subsequent reuse of information by third parties, even for commercial purposes. Not only the most common document management models and legal frameworks on technological innovation have considered information and data as a tool to meet the internal needs of the organisation, but they have usually ignored or underestimated potential subsequent reuse by third parties until very recently.[1] It is therefore essential to take the current reality as the starting point to assess the changes needed to move towards an innovative model of document management. A model that facilitates access to and reuse of administrative information based on the parameters of open data. As Osimo remarks, transparency can not only be a catalyst for e-Government but, above all, a catalyst for the transformation of the public sector as a whole.[2]

The initial push for the transformation of the regulation on access to public sector information came from the first EU legal framework on the reuse of administrative information, specifically, Directive 2003/98/EC of 17 November 2003. The aim was to promote the creation of a European-wide market for access to public-sector information, trying to overcome the barriers of a fragmented scenario by establishing homogeneous criteria, based on fair, proportionate and non-discriminatory requirements for the processing of information that can be reused.

While the European Union's competence in this area is indeed limited mostly to the promotion of said market, from the internal perspective of each Member State they are being forced to consider the political dimension of public-sector transparency as an unavoidable democratic requirement.[3] Moreover, the accessibility to information held by public bodies is becoming a requirement of the "right to know," as well as

* Article submitted to double-blind peer review.
This work is the result of the research project "Open Data and Reuse of Public-Sector Information in the Context of its Digital Transformation: Adapting to the New EU Regulatory Framework" (ref. PID2019-105736GB-I00), funded by the Spanish Ministry for Science and Technology (MCIN/AEI /10.13039/501100011033).

[1] S.S. Dawes and H. Helbig, *Information Strategies for Open Government: Challenges and Prospects for Delivering Public Value from Government Transparency*, in M.A. Wimmer, J.L. Chappelet, M. Janssen, and H.J. School (eds.), *Proceedings of the 9th IFIP WG 8.5 International Conference on Electronic Government*, Berlin-Heidelberg-New York, Springer, 2011, 58, who highlight the fact that this dimension involves taking on new functions that require not only greater investments but, above all, new skills and knowledge for government staff, as well as innovative policies and changes in administrative procedures and practices.

[2] D. Osimo, *Benchmarking eGovernment in the Web 2.0 Era: What to Measure and ow*, in *European Journal of ePractice*, 4, 2008, 33-43.

[3] A.G. Orofino, *La transparenza oltre la crisi. Accesso informatizzazione e controlo civico*, Bari, Cacucci, 2020, 237-246.

an opportunity to perform better control by society. From the perspective of *open data*, both considerations are equally legitimate and can no longer be seen as mutually exclusive but rather as two reinforcing approaches.

However, the final consolidation of this approach does not simply call for administrative information to be accessible by electronic means.[4] Data should also be available under certain conditions: automated processing must be enabled and unjustified restrictions for reuse should be avoided, particularly without charge or, where appropriate, taking into account the marginal cost of dissemination. In this respect, Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public-sector information (DRPSI) has been a major advance since, indirectly but significantly, implies document management to be carried out by public-sector entities according to the requirements of technological innovation.[5]

The evolution of the technological, social, and economic context itself demands a regulatory framework better adapted to the challenges faced by the European Union in a global scenario. As a reason for the necessary updating of the 2003 regulation, a clear reference was made to the adaptation of legal guarantees to the demands of competitiveness and innovation that arise from technologies such as Artificial Intelligence or the Internet of Things. Thus, the 2019 reform was intended to take a first step into the process of modernising the regulatory framework for open data and the reuse of public-sector information which is currently undergoing a major update within the so-called *European Data Strategy 2020*.[6]

Regarding the DRPSI, the main novelties include two new categories of data which regulation is certainly advanced: dynamic data, of great importance for Artificial Intelligence and smart cities, and high-value data, which can generate significant socio-economic and environmental impacts, boost innovative services, benefit many people or SMEs, as well as be combined with other data sets. In both cases, the European regulation is firmly committed to facilitating access to these data by establishing demanding conditions. It envisages making them available immediately after their collection, through appropriate APIs and, where suitable, enabling mass downloading. Even though the new regulation also stresses the importance of the principle of *open data by design and by default*, it does not imply that there is a clear obligation for public-sector bodies to make disproportionate efforts to adapt the information they hold following these formal requirements. Consequently, this lack of enforcement may be seen as a serious barrier regarding data availability for innovative purposes and digital transformation.

2. *Towards Data Spaces, a New Approach in the EU Legal Framework*

E-Government regulations have generally focused on document safeguards, without paying special attention to the relevance of data. Moreover, these rules are still mainly anchored in an *ad intra* view of document management despite the increasing importance of the *ad extra* dimension, especially since the consolidation of Open Government as one of the main axes of public policies.[7]

It is therefore not surprising that EU law has been the driving force behind a paradigm shift in regulation to a large extent. However, its key objective has not been so much to have a direct impact on the regulation of administrative activity but, on the contrary, to set the conditions for an EU-wide market for data, especially data generated by public bodies, with adequate safeguards for rights and freedoms. This purpose has now taken on a new significance, as digital context and technological innovation are largely based on

[4] Cf. B.S. Noveck, *Wiki Government. How technology can make government better, democracy stronger, and citizens more powerful,* Washington DC, Brookings Institution Press, 2009, 125.

[5] For an exhaustive analysis of this regulatory framework and the subsequent adaptation of Spanish legislation, see J. Valero Torrijos and R. Martínez Gutiérrez, (eds.), *Datos abiertos y reutilización de la información del sector público*, Granada, Comares, 2022.

[6] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* of 19 February 2020, COM(2020) 66 final.

[7] It is of great importance to insist on the need for a regulatory framework for administrative activity that would promote the demand for a data-driven orientation from the perspective of good regulation. On this idea, see D. Canals Ametller, *El acceso público a datos en un contexto de transparencia y buena regulación*, in D. Canals Ametller (ed.), *Datos. Protección, Transparencia y Buena Regulación*, Girona, Documenta Universitaria, 19-20.

the availability of enough and adequate data.[8]

Beyond the specific regulation on reuse and open data already referred to, the following pages will analyse the main milestones of the latest EU regulatory approach in this area - including the immediate future - and its potential impact on the regulation and practice of public-sector document management at a national level.

2.1. *The European Data Strategy*

The influence of the European Union in this area has been significantly strengthened with the *European Data Strategy*. This is a non-legislative document which main goal is for the EU to become a "role model of a society empowered by data to make better decisions, in business and the public sector." More precisely, it expresses the desire to "benefit from better use of data, including greater productivity and competitive markets, but also improvements in healthcare and well-being, environment, transparent governance, and convenient public services".

In terms of data availability, the *Strategy* no longer has its focus on data from the public sector, as it had been the case until now due to the prominence of the regulation on open data and its reuse, thus broadening the subjective perspective of its approach. Apart from exchanges between private parties, the need to optimise the collection of privately owned data by public bodies is raised to "improve evidence-driven policymaking and public services such as mobility management or enhancing the scope and timeliness of official statistics, and hence their relevance in the context of new societal developments".

Beyond the availability of data and, particularly, the technical conditions to ensure interoperability to facilitate the exchange, the *Strategy* poses two major challenges. On the one hand, it emphasises that "organisational approaches and structures (both public and private) that enable data-driven innovation on the basis of the existing legal framework are needed", from a cross-sectional perspective in particular. On the other hand, it highlights the importance of promoting a regulation that makes access to data more dynamic, not only in general terms of design and governance of relationships between private parties[9] but specifically in each of the data spaces.

2.2. *The Data Governance Act*

Unlike the 2019 DRPSI, *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724* (DGA) set up a legal framework that will be directly applied across the European Union as of 24 September 2023. This is intended to harmonise the EU's internal market facing the risk of unilateral regulation by Member States fragmenting it if there is not a common discipline to help boost cross-border digital services.[10] However, it respects the competence of each Member State regarding the organisational measures to be adopted and their right to legislate access to public-sector information.

This is an important shift that is becoming more widespread because of the latest regulatory initiatives promoted by the European Union in the digital environment. It confronts the problems generated by directives which, as is well known, requires further transposition activity by Member States. This approach seems to be strengthened with most of the regulations planned in this and similar fields: the Artificial Intelligence proposal, the so-called *Data Act* and, more recently, the proposal about sectoral regulation on the healthcare data space. As mentioned above, the rules included in a EU Regulation are directly applicable. Consequently, those provisions of national legislation on the use of electronic media, transparency or reuse of public-sector information that are contrary to its provisions would be displaced and, likewise, the interpretation of these State laws must facilitate the effectiveness of the European regulation.

[8] This is a particularly relevant premise in the case of Artificial Intelligence, to the extent that it may even generate a new gap between public administrations and public entities depending on the more or less advanced level of digitisation. In this regard, see J. Miranzo Díaz, *Inteligencia artificial y contratación pública*, in I. Martín Delgado and J.A. Moreno Molina (ed.), *Administración electrónica, transparencia y contratación pública*, Madrid, Iustel, 2020, 128.

[9] This idea has led to the *Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data* (*Data Act*) of 23 February 2022, COM(2022) 68 final.

[10] In any case, the implementation of this regulation may entail a bureaucratic and procedural complication, as has been accurately pointed out. On this issue, see S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, in *Rivista di Digital Politics*, 1-2, 2022, 194.

Secondly, it is a regulation that, as regards the reuse of public-sector information, includes complementary provisions to the DRPSI.[11] It is based on the observation that there are still major difficulties in facilitating access regarding certain special categories of data. Thus, a new regulation is established (Article 3) for those sets of data over which there are third-party rights that hinder their reuse, such as the protection of personal data,[12] intellectual property or, among other legal interests, statistical or commercial confidentiality. The concurrence of these legal barriers can seriously hinder - and even prevent - the reuse of data of enormous value when implementing projects of great impact in the current social and technological context, such as those related to research and those based on the innovation required by digital transformation. In this respect, data-driven document management would address this challenge, so that instead of providing access to documents as a whole, it would be possible to limit access to only part of them and even provide them in a dissociated manner, i.e., without linking them to any subject, thus overcoming the drawbacks posed by accessing formalised documents.

Taking these objectives and challenges into consideration, the initiative aims to lay the foundations for building a European data governance model based on transparency and neutrality, as a counterbalance to the trends emerging from other geographical, political and economic spheres. It is specifically considered to establish a regulatory framework that reinforces the confidence of citizens, companies, and other organisations in the fact that their data will be reused under minimum legal standards, thus facilitating control over third parties' usage. DGA regulations promote measures that ensure, on the one hand, the lawfulness of the reuse of data for purposes other than its primary use specifically the impact on the data subject and, on the other hand, it contemplates adequate mechanisms for the protection of their legal position.

The main novelties of the regulation include the following:

- the obligation for public bodies that allow the reuse of this type of data affected by the rights and interests of third parties to adopt the technical, organisational, and legal measures that guarantee their effective protection (Article 5.5 DGA);
- the power granted to public bodies to impose reuse under certain conditions, by requiring data to be subjected to a "pre-processing" process that consists of anonymisation, pseudonymisation or, where appropriate, deletion of confidential information (Article 5(3)(a) DGA);
- it is foreseen that reuse may only be allowed in environments controlled directly by the public body (Article 5.3.b DGA);
- and, finally, public bodies are granted the power to prohibit the use of those results of data processing that endanger the rights and interests of third parties (Article 5.4 DGA).

In short, the measures implemented by the DGA provide solutions specifically aimed at tackling the conflicts arising from access to public-sector data that could affect the legal position of third parties, incorporating mechanisms that provide greater legal certainty and, therefore, reinforce the confidence of the holders of the aforementioned rights and interests. However, its effective implementation requires data accessibility to be considered from design and by default and therefore considering this requirement when choosing or designing the document management model. Otherwise, the necessary additional data processing to overcome the legal barriers may make access almost definitively difficult, especially regarding the economic conditions.[13]

[11] P. Dopazo Fraguío, *El nuevo Reglamento europeo para la gobernanza del dato: ¿liberalización segura de información y neutralidad de su tratamiento*, in *Revista Española de Derecho Europeo*, 82, 2022, 143, 160.

[12] This has traditionally been one of the main legal difficulties in facilitating access to administrative information for reusing purposes. On this tension, see H. Graux, *Open Government Data: Reconciling PSI Reuse Rights and Privacy Concerns*, in *European Public Sector Information Platform Topic Report*, 2011/3, and Article 29 Data Protection Working Party, *Opinion 06/2013 on open data and public sector information ('PSI') reuse*, of 5 June 2013.

[13] In this sense, one of the main challenges posed by the opening of data by public bodies to facilitate their reuse relates to how to finance the necessary transformation of the information prior to making it available to third parties in formats that allow its reuse in an automated manner. On the risks and difficulties of each option, see A. Sánchez García, *El valor económico de la información pública y la regulación del precio de su reutilización*, in J. Valero Torrijos and R. Martínez Gutiérrez (ed.), *Datos abiertos y reutilización de la información del sector público*, Granada, Comares, 2022, 226-232.

2.3. *Data Spaces: A Complex Ecosystem of Advanced Document Management*

As mentioned above, the *European Data Strategy* envisages the launch of a series of data spaces to promote added-value services and products based on technological innovation. Although there is no general regulation, they are considered ecosystems where data from the public sector, companies and individuals, as well as research institutions and other types of organisations are available and exchanged reliably and securely.[14]

These spaces aim to promote scenarios where the voluntary sharing of participants' data can be implemented within an environment of sovereignty, trust, and security, through integrated governance, organisational, regulatory, and technical mechanisms.[15] Such spaces will allow participants to take on diverse roles, whether as data producers, data consumers, data service providers, component developers or operators of essential services.[16]

As far as public bodies are concerned, their position would be comparable to that of any private subject if they use the data or provide data-based services under the same conditions. However, these entities are above all called upon to play a key role from two points of view. Firstly, the public sector will often be the promoter or oversee the governance of the space, setting the conditions for all participants and, if necessary, enforcing them; so that if a public body provides its data and uses the data provided by others, the two roles should be separated into two different entities, to ensure the neutrality of the decisions to be taken.

Secondly, public-sector bodies have a particularly active role to play in the implementation of the legal provisions on reuse and open data as data spaces can be fed by the information they provide and by high-value data. That is, data must be made available by public entities under certain standards, namely: a machine-readable format, through APIs and, where appropriate, downloadable by bulk. These requirements oblige, on the one hand, to adopt technical, organisational, and legal measures to allow access to the data following them and, on the other hand, to make the data available from a single point of access regardless of whether the administrative competences in the respective field are spread over different territorial levels or are held by different entities. Consequently, the fragmentation of competences inherent to a decentralised State may involve a major barrier to the processing of data that, however, should not imply the need to resort to different data sources. On the contrary, integrated systems should be implemented *ad intra* based on inter-administrative relations according to interoperability requirements, so that access would be enabled through a single and integrated point.

These spaces represent an emerging model of public-private collaboration[17] but, even though there are already important initiatives underway, they currently lack a minimum of general regulation at EU level that could help us understand their scope. Nevertheless, as far as the subject of this paper is concerned, it is at least possible to draw some initial remarks that are useful when it comes to pointing out the consequences for document management in the public sector.

Data spaces involve a prominent role for public entities and demand a higher degree of integration with other subjects as well, particularly in the private sector. Consequently, an additional interoperability effort is required both from a technical/organisational perspective and a legal one; a requirement of great relevance as regards the conditions of access to information and the conditions of its reuse, since the diversity in the origin of the data also implies the heterogeneity in the applicable regulation. Even more, unless a clear legal provision is stablished, it would not be appropriate to impose certain conditions unilaterally and therefore, transparent, and participatory management models should be sought. In the end, a legal approach limited only to eGovernment, open data and reuse of

[14] European Commission, *Commission Staff Working Document on Common European Data Spaces*, 2022, 4.
[15] C. Alonso Peña, *Espacios de datos: visión conceptual y características*, *Boletic*, 91, 2022, 28.
[16] C. Alonso Peña, *Espacios de datos: visión conceptual y características*, 30.

[17] Although "cultivating engaging relationship with the public is challenging for government organizations, the negative consequences of government isolation from citizens are enormous" (VvAa., *Building Digital Government Strategies. Principles and Practices*, Cham, Springer, 2017, 110). This risk is particularly intense in digital scenarios, where complexity demands deeper co-operation with private entities.

information regulations, which are primarily designed for the public sector, would therefore not be enough.

2.4. *The Forthcoming European Regulation on the Health Data Space as an Example of the Need for a New Model of Governance*

One of the essential tools of the *European Data Strategy* refers to the creation of common and interoperable data spaces in strategic sectors at EU level, to overcome the legal, organisational, and technical obstacles to data sharing in specific areas of relevance. To this end, the *Strategy* envisaged a series of regulatory initiatives which, on the one hand, have materialised in the horizontal measures established in the DGA and, on the other hand, in the promotion of data spaces. In this respect, the Strategy provided for the possibility to complement this general regulation with sector-specific provisions on access to and use of data, as well as mechanisms to ensure interoperability.

Data access and exchange demand a more accurate approach that reflects the specificities of each field and the difficulties and challenges to be addressed. Considering the general regulatory framework referred to above, the Commission has presented a draft regulation on the European Health Data Space.[18] This initiative aims to boost data accessibility for primary uses, i.e., the provision of healthcare, while seeking to establish adequate conditions for secondary uses to promote new digital and innovative healthcare services and products. To this end, a unique governance model of its own, with a specific body at the helm is envisaged, the European *Health Data Space Board*, as well as the deployment of duly coordinated Member States administrative structures in charge of facilitating access to data.

In terms of the reuse of data for purposes other than healthcare, the proposed Regulation is based on the following evidence which, raises a general problem in many public entities: even though health data are already being collected and processed using electronic means, access to them is not always facilitated to fulfil other purposes of general interest.[19] With that in mind, the Regulation intends to promote a broad regulation that enables, among other purposes, the preparation of statistics, the development of training and research activities, such as technological innovation -including training of algorithms- or personalised medicine.

Regarding the parties obliged to share data, the proposed regulation applies to those who collect and process data with public funding, who must make them available to the competent bodies to facilitate their reuse. However, given their importance in some Member States, the regulation also extends its scope to private bodies providing healthcare services - unless they are micro-companies - and even to professional associations.

The regulation is based on a general rule: access to anonymised data to reduce privacy risks, although a specific regime is also envisaged for personal data. In this case, the request must include an adequate justification and the data will only be provided in pseudonymised form. Regarding access, the sensitivity of health data provides that they should be made available through a secure processing environment that complies with certain technical and security standards. In particular, the proposal does not allow data to be transmitted directly to the entity that will reuse them, except for non-personal data. Furthermore, it provides for processing to be carried out in secure environments under the control of access authorities.

From the perspective of the governance model underpinning the proposal, Member States should have at least one health data access body to provide electronic access for secondary purposes. In the case of several bodies due to requirements arising from their political-administrative organisation, one of them will exercise coordinating functions. Beyond the organisational freedom of the States to choose one or another formula, the independence of the coordinating body must be guaranteed, without prejudice to the mechanisms of financial or judicial control. In this respect, it is proposed that these bodies should be given the powers to verify compliance with these rules and to impose sanctions and other measures such as

[18] Proposal for a *Regulation of the European Parliament and of the Council on the European Health Data Space* of 3 May 2022, COM (2022) 197 final.

[19] However, disagreement has been expressed with the negative impact that the proposal could have by intensifying the fragmentation of the regulation given the numerous references it contains to the rules of the States. In this respect, see S. Navas Navarro, *Datos sanitarios electrónicos. El espacio europeo de datos sanitarios*, Madrid, Reus, 2023, 227, 228.

temporary or permanent exclusion from the European Health Data Space of those who do not fulfill their obligations.

The harmonisation sought by the proposed Regulation is also envisaged in the establishment of a standardised procedure for the issuing of permissions to reuse data. In cases where anonymised access to data is not enough, the applicant will have to justify why pseudonymised access is necessary. In the latter case, the request should specify the legal basis for requesting access to the data from a data protection perspective, the secondary purposes for which the data are intended to be reused, as well as a description of the data and tools necessary for their processing.

Finally, the proposal includes active publicity obligations addressed to the aforementioned bodies regarding the available datasets. This is an essential provision, since the existence of a catalogue of datasets at the European level - based on the interconnection of national datasets - would be extremely useful for promoting not only research and innovation but also decision-making at a regulatory, political and management level. For each set of available data specifically, the nature of the data, its source, and the requirements for making the data available shall be indicated.

The main purpose of this initiative is to ensure a uniform and consistent application of the regulatory framework for health data access for secondary purposes throughout the European Union, particularly regarding the protection of personal data. However, beyond the singularities in this field, this is an example that shows that document management of healthcare institutions – particularly public ones, in the case of the object of our work - must undergo a profound renewal, taking on the challenge that data can not only be used for healthcare purposes but be provided to third parties as well. It requires the adoption of management guidelines and criteria based on data and, specifically, on facilitating access to them from the design and by default requirements. Therefore, the mere digitalisation of documents is not enough and, for this reason, the limitations inherent in the regulation on e-Government, open data and reuse of public sector information should be overcome.

3. *The Challenges Ahead*

The approach of eGovernment regulation in the field of document management has been frequently characterised by a twofold perspective: on the one hand, by an outstanding and almost exclusive orientation towards documents and their mere digitisation and, on the other hand, by the almost irrelevant role that data have been playing, except for the latest reforms promoted by the European Union and, also, by the growing prominence of Open Government.

Consequently, these premises have substantially conditioned not only administrative practices but also the debate on the necessary adaptation of legal guarantees to the singularities of technological innovation.[20] This problem has become evident in recent times with the need for a management model based substantially on data, both in terms of better compliance with regulatory obligations and, given the need to have sufficient data, to meet the demands of technological innovation for the exercise of public functions, especially regarding Artificial Intelligence and, in general, the automation of administrative activity.

The commitment to an advanced and proactive model of document management in the public sector that faces those obstacles must be perceived as a strategic necessity that goes beyond mere compliance with current legal provisions. It is a challenge that must necessarily be addressed proactively, by design and by default, that is, using standards and approaches that allow the automated management of data without the need for additional processing, both in terms of their internal use for the exercise of public functions and, above all, from the perspective of their openness and reuse. Otherwise, it will not be possible to comply with the regulatory obligations in an efficient way and, more worryingly, it will not ensure adequate guarantees regarding the technical and legal conditions under which data must be kept, managed, and opened.

Moreover, the current complexity of digital environments determines that data generated

[20] It is therefore essential to adopt an approach based on services rather than on procedure, as suggested by I. Martín Delgado, *El acceso electrónico a los servicios públicos: hacia un modelo de Administración digital auténticamente innovador*, in T. De la Quadra Salcedo and J.L. Piñar Mañas (eds.), *Sociedad digital y Derecho*, Madrid, BOE-Red.es, 2018, 187-190.

by public-sector bodies must be integrated with data from other private sources, which requires an additional effort when establishing the conditions under which interoperability will take place, which can no longer be unilaterally defined by the public sector. Private entities are also called upon to play a relevant role, not only by facilitating access to their own data but, above all, by providing intermediation services with an unquestionable added value.[21] Consequently, it is necessary to promote alternative models that are legally adapted to the demands and singularities of digital and innovative ecosystems. In short, to go beyond regulatory obligations and assume advanced governance models[22] where data play the leading role they are entitled to.

[21] In the end, there is a clear need "for a coherent advancement of the regulatory framework with regard to data intermediaries, which would eventually contribute to an effective market design on data sharing" (H. Richter, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *GRUR International*, 72(5), 2023, 470). Moreover, intermediaries are even called upon to play an important role in the effectiveness of legal guarantees (M. von Grafenstein, *Reconciling Conflicting Interests in Data through Data Governance*, in *HIIG Discussion Paper Series*, 2022-02, 37), which again leads to the growing significance of governance models over and above regulation itself.

[22] On the scope of this concept from the perspective of data in the Spanish public sector, C. Ramió, *La década de la innovación en la gestión pública en España: una agenda para 2030*, in C. Ramió (ed.), *Repensando la Administración digital y la innovación pública*, Madrid, Instituto Nacional de Administración Pública, 2021, 62-64.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 43-50
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 05

*L'open data des collectivités territoriales entre gouvernance et souveraineté**

Jennifer Marchand
(Associate tenured professor at the University Clermont Auvergne)

ABSTRACT The development of open data within local authorities still suffers from difficulties in being put into practice for lack of a strategic framework and insufficient consideration of sovereignty issues. To make use of the data's potential, they must, at the same time, establish some tools prescribing governance and ensure full control over the data.

1. *Introduction*

L'ouverture des données publiques (« *open data* ») peut se définir comme la diffusion proactive, en accès libre et gratuit, de données produites par les administrations, sous un format numérique facilement réutilisable pour permettre leur appropriation par des tiers. Elle offre des opportunités considérables de création de valeurs - telles que la transparence[1] et l'efficacité de l'action administrative - et de développement de nouveaux usages et services[2]. Amorcée dans les années 70[3], la dynamique d'ouverture va s'accélérer et s'élargir. Depuis les années 2010, la France mène une politique active en la matière qui recouvre trois volets : 1°) un volet matériel avec la création de la plateforme ouverte et communautaire data.gouv.fr[4] ; 2°) un volet structurel avec la création de la direction interministérielle du numérique[5], dont le département Etalab assume le rôle de « Chief Data Officer » au titre des missions de l'Administrateur général des données[6] ; 3°) un volet juridique avec le code des relations entre le public et l'administration (CRPA), tel que modifié par la loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public et par la loi 2016-1321 du 7 octobre 2016 pour une République numérique. Le régime juridique de l'*open data* repose désormais sur une double logique[7]. Il favorise d'une part, l'accès aux informations contenues dans les documents administratifs[8] en consacrant l'ouverture par défaut des données détenues par les collectivités publiques sans attendre qu'un citoyen en formule la demande[9]. Il promeut d'autre part, la

* Article submitted to double blind peer review.

[1] H. Michel, *Promesses et usages des dispositifs de transparence : entre approfondissement et redéfinition de la démocratie*, in *Revue française d'administration publique* 2018, n° 1, 5-15.

[2] L. Cluzel-Métayer, *L'ouverture des données publiques*, in *Le Droit administratif au défi du numérique*, Paris, Dalloz, 2019, 7-23.
J. Marchand, *L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique*, in *Semaine Juridique Administrations et collectivités territoriales*, 17 février 2014, n° 7, n° 2038.

[3] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public (Journal officiel 18 juillet 1978). Elle crée la Commission d'accès aux documents administratifs (CADA), autorité administrative indépendante chargée d'assurer et contrôler l'accès des particuliers aux documents administratifs.

[4] www.data.gouv.fr/fr/pages/about/a-propos_data-gouv.

[5] Créée par le décret n° 2019-1088 du 25 octobre 2019 (Journal officiel n° 0251), la direction interministérielle du numérique succède à la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) créée dès 2011. Elle pilote notamment la mise en œuvre du volet Transformation numérique de l'État et des territoires dans le cadre du Plan France Relance.

[6] Fonction créée par le décret n° 2014-1050 du 16 septembre 2014 (Journal officiel n. 0215 du 17 septembre 2014). Pour relancer l'open data, chaque ministère doit désormais nommer un administrateur des données chargé d'élaborer la stratégie d'ouverture du ministère (circulaire n° 6264/SG du 27 avril 2021).

[7] L. Cluzel-Métayer, *Le code face aux données*, in G. Koubi, L. Cluzel-Métayer, W. Tamzini, *Lectures critiques du code des relations entre le public et les administrations*, 2018, Paris, Lextenso, 181-192.

[8] Les données sont intégrées à la notion de document administratif telle que définie à l'article L. 300-2 du CRPA. Sur le passage du document administratif à la donnée, voir G. Koubi *Équivoque administrative sur la donnée publique*, in *Semaine Juridique Administrations et Collectivités territoriales*, 2018, n° 18-19, 2142.

[9] J.-P. Foegle, *L'ouverture des données publiques à l'ère du numérique : de la demande à l'offre*, in *Revue du Droit public*, 2018, n° 3, 677.
L'ouverture par défaut concerne les documents communiqués à la suite d'une demande d'accès, les documents figurant dans les répertoires d'informations publiques, les bases de données mises à jour de façon

réutilisation gratuite et dans un format ouvert des données publiques. Lorsqu'elles constituent des données de référence, leur mise à disposition en vue de faciliter leur réutilisation constitue une mission de service public relevant de l'État[10].

Si les réformes législatives successives ont permis à la France de se positionner parmi les pays les plus avancés en matière d'ouverture des données[11], il convient de souligner que les collectivités territoriales ont grandement participé à ce succès. En ayant créé les tous premiers portails d'accès aux données, les collectivités territoriales doivent en réalité être considérées comme les pionnières de l'*open data*[12]. Les données générées par les nombreux services publics locaux (urbanisme, transport, voirie et stationnement, éclairage urbain, qualité de l'air et de l'eau, vidéoprotection…) représentent pour les collectivités une source d'information importante pour la connaissance de leur territoire et le pilotage de leurs politiques. L'*open data* des données territoriales constitue l'un des instruments pour améliorer la gestion des services publics locaux[13] en concrétisant les lois du service public telles que la mutabilité, la continuité ou encore la qualité[14]. En tant qu'indicateur de performance, la donnée contribue à une plus grande efficacité des politiques publiques locales par l'établissement d'instruments de suivi du taux de réalisation ou d'exécution des actions et projets mis en œuvre. À ce titre, « les politiques d'*open data* constituent une ressource de communication non négligeable pour les élus locaux […] et dessinent la figure de l'élu réformateur[15] ». La politique d'ouverture est en outre un élément essentiel pour le développement des projets de territoires intelligents. De nombreux cas d'usage de la donnée publique ouverte sont ainsi développés par les collectivités territoriales (mais aussi par les opérateurs privés délégataires ou non de service public) dans les domaines de la mobilité, de l'énergie, de l'eau et des déchets. La donnée apparaît alors comme le substrat d'une nouvelle politique territoriale porteuse d'opportunités pour les collectivités et leurs habitants[16].

Les potentialités d'innovation attachées aux données publiques semblent partagées par l'ensemble des acteurs publics. Or, les statistiques démontrent que si, la politique *open data* progresse dans les collectivités, ce n'est que dans des proportions modestes ou inégales. Selon l'Observatoire open data des territoires[17], en 2021, 715 collectivités (communes, EPCI, départements et régions) ont ouvert leurs données soit une progression de 21% par rapport à l'année précédente. En réalité, cela ne concerne que 14% des collectivités visées par la loi pour une République numérique[18] mais couvre néanmoins 50% de la population. Dans le détail, deux tendances ressortent de la lecture de ces chiffres. Le mouvement d'ouverture lorsqu'il est initié, ne l'est que dans des proportions très limitées. 41% des collectivités ne publient qu'un ou deux jeux de données. Il existe par ailleurs un effet de seuil et de fortes disparités selon la taille de la collectivité. Si l'intégralité des régions, deux tiers des départements et plus de la moitié des communes et EPCI de plus de 100 000 habitants ont ouvert leurs données, seulement 10 % des plus petites collectivités ont initié une politique d'ouverture. La fusion des régions et le renforcement de la coopération intercommunale ont accéléré au sein de ces collectivités la fusion des systèmes

régulière et les données mises à jour de façon régulière dont la publication présente un intérêt économique, social, sanitaire ou environnemental (article L. 312-1-1 du CRPA).

[10] Article L. 321-4 du CRPA.

[11] *Pour une politique publique de la donnée*, rapport d'étude remis au premier ministre par la mission Bothorel, décembre 2020, p. 66

[12] S. Manson, *La mise à disposition de leurs données publiques par les collectivités territoriales*, in *Actualité juridique Droit administratif*, 2016, n° 2, 97.

[13] Voir par exemple, le projet expérimental de plateforme collaborative France data réseau qui permet aux collectivités de partager leurs données liées aux activités des services publics locaux en réseau (FNCCR, actualités, 24 févr. 2022 : www.fnccr.asso.fr/article/partager-les-donnees-territoriales-pour-ameliorer-les-services-publics).

[14] L. Cluzel-Metayer, *Le service public et l'exigence de qualité*, Paris, Dalloz, 2006.

[15] S. Manson, *La mise à disposition de leurs données publiques par les collectivités territoriales*, 98.

[16] L. Bélot, *De la smart city au territoire d'intelligence(s)*, rapport au Premier ministre, avril 2017.

[17] www.opendatafrance.net/wp-content/uploads/2021/12/Observatoire-ODT-2021-v1.1-17dec21.pdf.

[18] Les collectivités territoriales de plus de 3500 habitants (soit un total de plus de 4600 collectivités) sont directement visées par l'article L. 312-1-1 du CRPA et sont à ce titre soumises au principe de mise à disposition spontanée des données publiques. Dans le même sens : article L. 1112-23 du Code général des collectivités territoriales (CGCT).

d'information, le remplacement progressif des portails par des plateformes *open data*[19], le recentrage sur la réutilisation et le contrôle des données publiques territoriales[20]. En revanche, pour les collectivités de plus petite taille, l'*open data* n'est pas une priorité en raison d'un manque de moyens humains et techniques et d'une méconnaissance des données produites sur leur territoire. Dans ce contexte, les grandes collectivités sont amenées à jouer un rôle moteur dans la promotion et le développement de l'*open data*. Elles accompagnent, avec une logique de mutualisation, les plus petites collectivités dans le mouvement d'ouverture des données lequel n'a de sens que s'il est collectif et communément partagé par l'ensemble des acteurs et échelons territoriaux[21].

Plus de dix ans après la mise à disposition des premiers jeux de données publiques, certains regrettent toujours l'absence d'une véritable politique publique de la donnée. Le niveau de maturité général des collectivités territoriales sur la donnée demeure globalement faible. Le déploiement de l'*open data* au sein des collectivités territoriales pâtit encore de difficultés de mise en œuvre[22] faute d'un cadre stratégique et d'une insuffisante prise en compte des enjeux de souveraineté. Pour exploiter au mieux le potentiel des données, les collectivités doivent par conséquent se doter d'une part, d'une gouvernance de la donnée prescriptrice d'outils et de méthodes (2) et d'autre part, s'assurer de la pleine maîtrise des données (3)

2. *La gouvernance des données publiques locales*

La gouvernance des données se définit comme un « ensemble de principes et de pratiques qui visent à assurer la meilleure exploitation du potentiel des données[23] ». Pour les collectivités territoriales, la gouvernance suppose d'élaborer une doctrine sur les données produites et collectées, de déterminer les usages qu'elles souhaitent promouvoir et de se doter d'outils au service d'une stratégie centrée sur la donnée. La gouvernance est le préalable nécessaire à toute politique *open data*. Elle revêt habituellement deux dimensions[24] : interne avec le déploiement d'un management de la donnée (2.1.) et externe avec une animation territoriale de la donnée (2.2.).

2.1. *La gouvernance interne des données publiques locales*

L'organisation administrative des collectivités territoriales se caractérise bien souvent par une structuration en silo selon laquelle chaque service centré sur une mission ou une compétence fonctionne de manière autonome, sans lien ni partage d'information avec les autres services. Or, un tel fonctionnement s'oppose à la nature transversale de la politique d'*open data*. Instrument de la modernisation et de la transformation numérique de l'action publique, thématiques bien connues de la science administrative, l'*open data* modifie les principes d'organisation et les modes d'action des collectivités publiques. La gouvernance de la donnée va alors impliquer un décloisonnement et un management moins vertical[25]. Plusieurs choix s'offrent aux collectivités territoriales : la création d'un *chief data officer*, la mise en place d'un comité data, la nomination d'un référent data ou encore le recrutement d'un chargé de mission[26]. L'objectif est alors de faire de la

[19] Par exemple, la plateforme Opendata.clermontmetropole.eu est alimentée par les communes membres de Clermont Auvergne Métropole mais aussi par des acteurs du territoire qui souhaitent diffuser leurs données.

[20] Fédération nationale des collectivités concédantes et régies (FNCCR) – Caisse des dépôts, *Collecte et gestion des données numériques pour le pilotage des politiques publiques. Vers un big data territorial*., Novembre 2016, en ligne : www.fnccr.asso.fr/article/big-data-territorial-publication-de-letude-de-la-fnccr.

[21] A. Léchenet, *Les grandes collectivités locomotives de l'open data*, in *La Gazette des communes*, 20 août 2021.

[22] B. Delaunay, *L'open data dans les collectivités territoriales*, in *Semaine Juridique Administrations et Collectivités territoriales*, 22 octobre 2018, n° 42, 2286.

[23] Administrateur général des données, rapport au Premier ministre sur la gouvernance de la donnée 2015 – *Les données au service de la transformation de l'action publique,* 73.

[24] La dichotomie gouvernance interne/gouvernance externe est empruntée au guide élaboré par la Banque des territoires (Caisse des dépôts et consignations) pour accompagner les collectivités territoriales dans la gestion de leurs données : *Gestion des données : quels outils et quelle stratégie pour les territoires ?*, janvier 2021 (www.banquedesterritoires.fr/gestion-des-donnees-territoriales).

[25] M.-A. Le Breton, H. Bailleul, J.-B. Le Corf et B. Mericskay, *La gouvernance des données urbaines entre territoire de projets et projets de territoire. L'exemple de Rennes Métropole*, in *Flux* 2022/1, 65-84, spéc. 71.

[26] Open Data France, *Le mois de la donnée : la gouvernance de la donnée*, 21 mars 2022, https://opendatafrance.gitbook.io/le-mois-de-la-data/gouvernance-des-donnees.

data, une fonction centrale et identifiée au sein de la collectivité et de parvenir à l'articuler avec les métiers et service existants (DSI, SIG) impliqués dans le « cycle de vie de la donnée ». Ce faisant, l'*open data* contribue à définir les contours d'une organisation administrative en « réseau et plus collaborative[27] ». Cette nouvelle structuration se heurte toutefois à un manque d'expertise. L'*open data* reste trop souvent une affaire d'initiés. La gouvernance nécessite alors un plan de formation des agents et le développement d'une culture de la donnée afin de contribuer à une montée en compétences collective. Certaines collectivités territoriales font le choix par exemple de mettre un place un comité de pilotage (COPIL) open data pour impliquer pleinement les acteurs locaux dans la démarche d'ouverture. D'autres organisent des sessions de formation (datalab ou hackathon). L'acculturation à la donnée publique et la sensibilisation aux enjeux de l'*open data* sont sans conteste les fondements d'une gouvernance interne réussie.

La gouvernance interne suppose également de définir une architecture susceptible de mieux tirer profit des données à disposition. Valoriser les données en *open data* nécessite de la part des collectivités territoriales de réaliser un travail d'identification et de recensement de leur stock de données[28]. Par la suite, un travail de modélisation et de cartographie mais aussi l'élaboration de référentiels permettront de standardiser la façon dont les services peuvent collecter, traiter et utiliser les données mais également favoriser une éventuelle réutilisation[29]. *In fine*, la gouvernance doit aboutir à la mise en place d'une infrastructure des données publiques incluant la création d'une plateforme de gestion et de partage des données territoriales[30] et véhiculer un ensemble de règles pour permettre un bon usage des données au sein de la collectivité. Il s'agit plus que jamais d'intégrer les données à un vaste écosystème[31].

2.2. *La gouvernance externe des données publiques locales*

La gouvernance externe, sans doute la plus complexe à mettre en œuvre, se caractérise par le déploiement d'une animation territoriale de la donnée en direction à la fois des collectivités territoriales, des citoyens et du secteur privé. La gouvernance consiste ainsi à structurer et animer une « communauté » territoriale autour de la donnée reposant sur la coopération, la mutualisation et des partenariats fondés sur le principe de subsidiarité[32]. Des collectivités territoriales voisines peuvent par exemple mettre en commun leur expérience et leurs bonnes pratiques, fédérer des actions conjointes ou conduire des projets partagés autour de la donnée. L'animation territoriale de la donnée peut alors se concrétiser de multiples façons à l'instar des initiatives déclinées dans le guide de la donnée élaboré par la région Bourgogne Franche-Comté[33] : mutualiser les données pour répondre à des préoccupations ou projets communs ; échanger les bonnes pratiques, les savoir-faire et les retours d'expérience ; échanger les données entre collectivités voisines ; mutualiser les plateformes *open data*. La gouvernance externe des données publiques locales contribue en outre à dépasser les limites territoriales dans une

[27] J. Chevallier, *Vers l'État-plateforme ?*, in *Revue française d'administration publique*, 2018, n° 3, 627-637, spéc. 634.

[28] Les premiers recensements à opérer concernent les données personnelles au titre de la mise en conformité RGPD puis de manière coordonnées les jeux de données essentielles choisis pour une publication en *open data*. Voir J. Marchand, *La protection des données à caractère personnel : quels risques pour les collectivités territoriales ?*, in *Semaine Juridique Administrations et collectivités territoriales*, 22 octobre 2018, n° 42, 2287.

[29] La Banque des Territoires (Caisse des dépôts et consignations) a fait réaliser en 2020 un recensement de toutes les grandes familles de données produites dans le cadre de la mise en œuvre des politiques publiques locales. Ce recensement rassemble 148 familles de données qui correspondent à 33 grands métiers territoriaux. Que ces données soient produites par les collectivités directement ou des entreprises agissant pour leur compte, le recensement est complété d'indications concrètes sur l'existence ou non de formats de données à respecter : www.banquedesterritoires.fr/smart-city-linnovation-au-service-des-territoires.

[30] Exemple du portail RUDI crée par la métropole de Rennes : https://rudi.datarennes.fr/presentation-du-projet.

[31] L. Cluzel-Métayer, *La loi pour une République numérique : l'écosystème de la donnée saisi par le droit*, in *Actualité Juridique Droit administratif*, 2017, n° 6, 340.

[32] Voir par exemple, les Trophées open data (édition 2019) parmi lesquels le « Prix de l'animation locale » a été attribué au Conseil régional d'Occitanie qui a su mener un vaste projet d'accompagnement des collectivités de la région.

[33] Région Bourgogne Franche-Comté, Parcours data, Le guide de la donnée accessible en ligne : www.bourgognefranchecomte.fr/sites/default/files/2022-01/Guide_DATA_Region_BFC_web.pdf.

perspective de solidarité. Nombreuses sont les initiatives portées par les collectivités pionnières en matière d'*open data* pour aider d'autres collectivités avec pour volonté, d'associer à l'ouverture des données, une politique de développement territorial. En la matière, « le niveau d'engagement semble être plus élevé dans les territoires où des initiatives de mutualisation, de mise en réseau, d'animation ou d'accompagnement ont réussi à créer une dynamique d'entraînement[34] ».

L'animation territoriale suppose également de stimuler la réutilisation des données publiques. L'open data ne peut pleinement se déployer que dans la mesure où c'est une démarche partagée. Le mouvement d'ouverture transforme les relations avec les citoyens et le secteur privé et interroge les modes de production des activités d'intérêt général. L'ouverture des données publiques favorise la co-innovation avec le secteur privé. Le partenariat consiste alors à reconnaître aux collectivités publiques le soin d'impulser l'innovation en externalisant les données publiques et de laisser le soin aux partenaires privés de proposer de nouveaux services. Les collectivités publiques endossent alors le rôle de stratège intéressé à l'édification d'un écosystème pourvoyeur de croissance[35].

3. *La souveraineté des données publiques locales*

Accaparées par la mise en œuvre de l'ouverture par défaut des données publiques, les collectivités territoriales n'ont pas, dans un premier temps, perçu les enjeux suscités par la problématique de la souveraineté des données. Or, cette dernière est prégnante. La souveraineté des données doit se comprendre comme le moyen pour les collectivités de conserver la maîtrise et le contrôle de leurs données et de celles que les acteurs privés (délégataires de service public) génèrent sur leur territoire. La souveraineté recouvre notamment la maîtrise du cadre juridique s'appliquant aux données. Deux instruments classiques du droit administratif[36] peuvent alors être utilement mobilisés : le service public pour assurer la maîtrise de la qualité de la donnée (3.1) et le contrat pour assurer la maîtrise de la propriété de la donnée (3.2).

3.1. *Le service public de la donnée*

La loi pour une République numérique du 7 octobre 2016 consacre le service public de la donnée dont les contours ont été précisés par le décret n° 2017-331 du 14 mars 2017. L'objectif du service public de la donnée est d'organiser la production, la qualité et la circulation des données de référence en garantissant un niveau de qualité minimale dans leur diffusion. Dans un univers de données très dense, il s'agit d'identifier des données de référence[37] c'est-à-dire des données « pivot », fiables et authentifiées par la puissance publique. L'identification d'un service public repose en droit français sur un critère formel, une intention, une manifestation de volonté de la personne publique d'assumer une activité d'intérêt général en tant que service public[38]. Si ériger la mise à disposition des données de référence en mission de service public témoigne de l'importance que revêt cette activité, un tel choix est surtout significatif « d'une volonté de la puissance publique d'assumer la maîtrise de la satisfaction d'un besoin qu'elles considèrent d'intérêt général et pour lequel elle juge l'initiative privée sinon totalement, au moins partiellement inadaptée[39] ». Pour préserver sa « souveraineté informationnelle[40] » ou sa « souveraineté numérique[41] », l'État doit conserver un

[34] "Open data : moins de 8% des collectivités locales ont ouvert leurs données publiques", *Maire-info*, édition du 11 octobre 2018.
[35] J. Marchand, *L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique*, 2038.
[36] J.-B. Auby, *Le droit administratif face aux défis du numérique*, in *Actualité juridique Droit administratif*, 2018, n°15, p. 835-844.
[37] Article L. 321-4 du CRPA. À ce jour, neuf jeux de données ont été identifiés comme des données de référence : la Base Adresse Nationale (BAN), la Base Sirene, le Code Officiel Géographique (COG), le Plan Cadastral Informatisé, le Registre parcellaire graphique, le Référentiel de l'organisation administrative de l'Etat, le Référentiel à grande échelle (RGE), le Répertoire national des association (RNA), le Répertoire Opérationnel des Métiers et des Emplois (ROME).
[38] Sur la conception subjective du service public : « Sont uniquement, exclusivement services publics les besoins d'intérêt général que les gouvernants, dans un pays donné, ont décidé de satisfaire par le procédé du procédé service public » (G. Jèze, *Principes généraux du droit administratif*, Tome II, Paris, Dalloz, 2005, p. 16).
[39] L. Cluzel-Metayer, *La construction d'un service public de la donnée*, in *Revue française d'administration publique*, 2018, p. 491-500, spéc. 492.
[40] Administrateur général des données, *rapport au Premier ministre sur la gouvernance de la donnée dans les administrations 2017 – La donnée comme infrastructure essentielle*, p. 16.
[41] H. Verdier, *Penser la souveraineté numérique pour*

pouvoir de direction stratégique c'est-à-dire la pleine maîtrise de la qualité de la donnée et ainsi éviter qu'elle ne perde son statut de référentiel dans le mouvement de réutilisation que promeut l'*open data*. Le service public de la donnée devient emblématique d'un modèle de société au sein duquel l'État est en capacité de réguler l'usage des données.

Les collectivités territoriales concourent au service public de la donnée par la production de données intégrées dans des bases nationales mais elles ne sont pas tenues de produire de nouvelles données. Elles doivent simplement améliorer la qualité des données qu'elles transmettent à l'État[42]. Certaines collectivités, comme la métropole de Rennes, ont néanmoins décidé d'aller plus loin en identifiant leurs propres données d'intérêt territorial lesquelles recouvrent pour Rennes, les données de référence (bases géographiques, bâtiments…), les données utiles au service public et les données du territoire[43]. La collectivité a ensuite créé un service public métropolitain de la donnée (SPMD). « Dédié à accompagner l'évolution des services publics, dans un environnement où les données prennent une importance croissante, le SPMD assure une mission d'intérêt général dans la production, la circulation, l'exploitation et le partage des données sur le territoire de Rennes Métropole[44] ». La collectivité se dote alors d'un instrument lui permettant de maîtriser la donnée en garantissant le respect de la confidentialité, la sécurité et la qualité de la donnée tout en en favorisant l'accès et la réutilisation. Ce faisant, elle se place en animateur et en garante des usages des données d'intérêt général produites sur son territoire. D'autres métropoles comme Brest se sont également lancées dans la création de leur propre service public de la donnée[45].

3.2. *Les clauses « open data »*

La question du partage et du retour « de certaines données fines à l'acteur public pour des missions de service public[46] » se pose à l'aune du pouvoir de direction qu'exercent les collectivités sur toute activité de service public même déléguée[47]. La collectivité doit pouvoir demander à conserver un droit de regard sur les données essentielles au fonctionnement du service public. Il y a là un enjeu de souveraineté. Or, les collectivités délégantes se sont longtemps heurtées au refus des délégataires et concessionnaires de leur communiquer, à l'issue du contrat, les données et bases de données constituées au cours de l'exécution du service public. Pour répondre à cette difficulté, l'article L. 3131-2 du code de la commande publique, issu de la loi du 7 octobre 2016 pour une République numérique, prévoit désormais que « lorsque la gestion d'un service public est concédée, le concessionnaire fournit à l'autorité concédante, sous format électronique, dans un standard ouvert librement réutilisable et exploitable par un système de traitement automatisé, les données et les bases de données collectées ou produites à l'occasion de l'exploitation du service public faisant l'objet du contrat et qui sont indispensables à son exécution ». Cette disposition à une double vocation : d'une part, assoir le pouvoir de contrôle de la collectivité concédante en tant qu'autorité organisatrice et s'assurer qu'elle dispose de « tous les éléments requis pour assurer la continuité du service public[48] » et développer l'ouverture de données essentielles relatives aux conditions d'exploitation du service public d'autre part[49].

une autonomie stratégique ? , in *Zdnet.fr*, 12 novembre 2020.

[42] Étude d'impact du projet de la loi pour une République numérique (NOR : EINI1524250L/Bleue).

[43] L'initiative est encouragée, voir notamment Institut Montaigne, "Villes, à vos données ! ", rapport 2021.

[44] https://rudi.datarennes.fr/wpcontent/uploads/2021/01/WEB_112017_Bilan_SPMD_A4_pages.pdf.

[45] *La métropole de Brest prépare son service public de la donnée*, in *La Gazette des communes*, 4 juin 2021.

[46] L. Archambault et C. Rotily, *Smart cities : les outils d'une révolution juridique maîtrisée*, in *Dalloz IP/IT*, 2021, p. 327.

[47] L. Bahougne, *Identification du service public*, in *Répertoire de service public*, Dalloz, juin 2021 : « Même en le déléguant, la personne publique n'abandonne jamais le service public. Elle conserve un " droit de regard " sur l'activité. Elle en conserve toujours la haute gestion Ainsi la gestion du service public est-elle objectivement distincte de la direction du service public par la personne publique ».

[48] J.-D. Dreyfus, *L'obligation du concessionnaire quant aux données et bases de données collectées ou produites à l'occasion de l'exploitation du service public. Open data et gestion des services publics*, in *Actualité juridique Collectivités Territoriales*, 2017, 187.

[49] Réponse ministérielle n° 13693, Journal officiel Sénat, 12 mars 2020, p. 1270 (en réponse à la question posée le 9 janvier 2020 par M. Claude Raynal) : « la qualification de bases de données indispensable n'empêche pas celle de biens de retour. Ainsi, d'une part, pendant l'exécution du contrat, les bases de données indispensables à l'exécution du contrat doivent faire l'objet d'une transmission à l'autorité concédante. D'autre part, à l'instar des autres biens meubles et

Cette disposition se combine avec celles relatives aux biens de retour favorisant ainsi une entière maîtrise de la collectivité sur ces données pendant et à l'issue du contrat. Les biens des contrats de délégation de service public et de concession repose sur une trilogie classique consacrée par le Conseil d'État dans l'arrêt Commune de Douai[50] et désormais codifiée à l'article L. 3132-4 du Code de la commande publique. Les meubles ou immeubles, qui résultent d'investissements du concessionnaire et sont nécessaires au fonctionnement du service public sont des biens de retour et restent la propriété de la personne publique dès leur réalisation ou leur acquisition. Lorsqu'ils ne sont pas remis au concessionnaire par l'autorité concédante et qu'ils ne sont pas indispensables au fonctionnement du service public, ils sont qualifiés de biens de reprise, propriété du concessionnaire, sauf stipulation contraire. Les biens qui ne répondent à aucune des deux définitions précédentes sont des biens propres qui demeurent la propriété du concessionnaire. Les données et bases de données produites par le concessionnaire privé, indispensables à l'exécution du service public, sont des biens de retour qui doivent, à l'instar de ce qu'a récemment reconnu le Conseil d'Etat pour les pages des réseaux sociaux[51], revenir à la collectivité concédante afin qu'elle ait en main tous les éléments pour préserver la continuité et les intérêts du service public[52]. Il reste néanmoins une interrogation. Comment s'assurer du respect des dispositions du Code de la commande publique et « contraindre les personnes privées à partager leurs données au motif qu'elles revêtent un caractère d'intérêt général ? [53]». Selon le rapport Bothorel, « la majorité des collectivités territoriales n'accèdent qu'à des données parcellaires et selon des modalités décevantes. Cette fourniture pour le moins limitée de données serait en effet la pratique la plus courante des concessionnaires[54] ». Plusieurs pistes sont possibles pour assurer l'effectivité de la loi et garantir un meilleur partage des données d'intérêt général au niveau territorial : favoriser l'incitation et encourager le partage des données à des fins altruistes à l'image du règlement sur la gouvernance des données (Data Governance Act[55]) ou insérer plus systématiquement dans les contrats une clause « open data ». La Banque des Territoires a ainsi récemment mis à disposition des collectivités territoires une boîte à outils et un guide sur les bonnes pratiques contractuelles proposant des clauses type[56]. Pour garantir la

immeubles, les bases de données qui constituent des biens de retour par détermination du contrat ou parce qu'elles résultent d'investissement et sont nécessaires au fonctionnement du service public sont, sauf stipulation contraire, la propriété de l'autorité concédante dès leur réalisation ou acquisition ».

[50] CE, ass., 21 décembre 2012, n° 342788, *Commune de Douai*, *Lebon* 477, conclusions Dacosta.

[51] CE, 16 mai 2022, n° 459904, *Commune de Nîmes c/ Société Culturespaces Lebon* 127, conclusions M. Pichon de Vendeuil.

[52] D. Pradines, T. Janicot, *Quand le « retour fait aimer l'adieu ». Dernières précisions sur l'application du régime des biens de retour*, in *Actualité Juridique Droit administratif*, 2022, 1204, commentaire sous CE, 16 mai 2022, n° 459904, *Commune de Nîmes c/ Société Culturespaces*.

[53] Anne Danis-Fatôme, *Quels garde-fous pour le partage des données*, in *Communication Commerce électronique* n° 5, Mai 2022, commentaire n° 37.

[54] *Pour une politique publique de la donnée*, rapport d'étude remis au premier ministre par la mission Bothorel, 183.

[55] Règlement du Parlement européen et du Conseil portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données). L'altruisme des données concerne les individus et les entreprises qui donnent leur consentement de mettre à disposition des données qu'elles génèrent — volontairement et sans récompense — pour être utilisées dans l'intérêt public. Les entités qui mettent à disposition des données pertinentes fondées sur l'altruisme en matière de données pourront s'enregistrer en tant qu'« organisations altruistes de données reconnues dans l'Union ». https://digital-strategy.ec.europa.eu/fr/policies/data-governance-act-explained.

[56] La Banque des Territoires (groupe Caisse des dépôts), *Guide des bonnes pratiques contractuelles et recommandations*, 2021, 10 : pour les concessions : « Les données produites, collectées, traitées ou gérées par l'autorité concédante ou par le concessionnaire pour son compte, dans le cadre de ses activités de service public et en lien avec ses compétences, en ce qu'elles sont nécessaires au fonctionnement du service public, constituent des biens de retour et sont réputées appartenir à l'autorité concédante dès l'origine. Le concessionnaire s'engage à permettre à l'autorité concédante d'accéder librement à ces données à tout moment de l'exécution du contrat. À l'issue de la concession, le concessionnaire s'engage à remettre gratuitement à l'autorité concédante toutes les données visées au premier alinéa du présent article et à apporter la preuve de leur destruction ». Pour les marchés publics : « Les données produites, collectées, traitées ou gérées par l'acheteur public ou par le titulaire du marché pour son compte, dans le cadre de ses activités de service public et en lien avec ses compétences, en ce qu'elles sont nécessaires au fonctionnement du service public, sont réputées appartenir à l'acheteur public dès l'origine. Le titulaire du marché s'engage à permettre à l'acheteur public d'accéder librement à ces données à tout moment de l'exécution du marché public. À l'issue du marché public, le titulaire du marché s'engage à remettre gratuitement à l'acheteur public toutes les

propriété des données, le contrat de concession pourrait contenir une clause réaffirmant que l'autorité concédante dispose d'un droit d'accès aux données nécessaire au fonctionnement du service public tout au long de l'exécution du contrat et qu'au terme de ce dernier, lesdites données reviennent gratuitement à la personne publique et doivent être détruites par le concessionnaire. Cette clause pourrait être déclinée dans les marchés publics. Pour les données d'intérêt général produites par des acteurs privés, certaines métropoles, ont inscrit dans une charte de la donnée une clause affirmant que « lorsqu'il est de l'intérêt de tous que les données privées d'intérêt métropolitain soient partagées avec la puissance publique parce qu'elles peuvent contribuer à la mise en œuvre des politiques publiques du territoire, la collectivité propose un cadre de dialogue avec les acteurs concernés pour créer les conditions d'un accès à ces données respectueux des droits de tous[57] ». Ces clauses et plus globalement l'outil contractuel permettent aux collectivités d'encadrer l'usage des données sur leur territoire et de conserver leur souveraineté sur des données essentielles[58] qui peuvent être considérées comme des biens communs eu égard à leur utilité collective[59].

4. *Conclusion*

Les questionnements entourant la gouvernance et la souveraineté des données publiques des collectivités territoriales peuvent sembler vertigineux. Ils sont en réalité à la hauteur des opportunités et des attentes entourant *l'open data* pour le développement des territoires. Les collectivités font souvent preuve d'inventivité sur un sujet technique devenu éminemment politique. Les outils juridiques, en particulier, s'adaptent et le droit de la donnée, en général, se développe pour inventer de nouveaux cadres d'échange de données fondés sur une gouvernance partagée et une maîtrise publique renforcée sur l'usage[60] des données d'intérêt territorial.

données visées au premier alinéa du présent article et à apporter la preuve de leur destruction ».

[57] https://metropole.nantes.fr/files/pdf/numerique-innovation/Charte-donnee.pdf.

[58] J.-D. Dreyfus, *L'obligation du concessionnaire quant aux données et bases de données collectées ou produites à l'occasion de l'exploitation du service public. Open data et gestion des services publics*, 187 : « les données d'intérêt général sont au moins aussi étroitement liées au service public que les informations qualifiées de données publiques. (...) il s'agit ici d'ouvrir l'accès aux données émanant de personnes publiques et privées, concessionnaires ou entités subventionnées par la puissance publique ».

[59] Les données peuvent être qualifiées de *« biens communs »* ce qui justifie leur ouverture : A.-S. Epstein, *Vers un droit d'accès du public aux données d'intérêt commun*, in J. Rochfeld, M. Cornu et G. Martin (dir.), *L'échelle de communalité: propositions de réforme pour intégrer les biens communs en droit*, Paris, Mission de recherche droit & justice, 2021, 342.

[60] A. Camus, *La propriété des données publiques*, in *Revue française d'administration publique*, 2018, n° 3, 479-490, spéc. 487-488 : « La maîtrise de l'administration ne porte pas directement sur les données publiques, mais sur leurs usages. La maîtrise des utilités des données publiques prend surtout racine dans le contrôle exercé par l'administration, en amont et en aval de l'usage ».

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 51-54
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 0.53136/9791221807981 06

*Openness of Public Data and Transparency of Administrative Action**

Angelo Giuseppe Orofino
(Full Professor of Administrative Law at Lum Giuseppe Degennaro University)

ABSTRACT This article has a two-fold objective: (i) firstly, it aims to present the main features of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union; (ii) secondly, it seeks to reflect on how those may affect public administrations – one of the most relevant players in the European data economy.

1. *Transparency as an Instrument of Administrative Democracy*

It has become essential to guarantee transparency in public action and in the way administrations carry out their functions. This necessity is the result of the legal and social evolution that has characterised certain Western European countries, such as Italy,[1] Spain,[2] France[3] and, to a lesser extent, Germany.[4] These countries, unlike the Anglo-Saxon[5] or Scandinavian states,[6] did not in the past have regulations implementing general measures of administrative transparency.

Over the last ten years, various laws and regulations have been enacted to strengthen administrative transparency and encourage citizen participation. This movement, which led to an 'explosion' of transparency[7] regulations, has overturned legal traditions based on the secrecy and impenetrability of public authorities.

The year 2013 seems to have been pivotal in this area, with the enactment of Spanish law no. 19/2013 of 9 December 2013, entitled 'Transparencia, acceso a la información pública y buen gobierno', and the adoption in France of loi organique no. 2013-906 of 11 October 2013 concerning 'Transparence de la vie publique'.

The year 2013 was important even in Italy because the government enacted a legislative decree concerning administrative transparency.[8] This decree was approved following a path which timidly began in 2009 with the 'Brunetta' reforms.[9] The legislative decree was adopted on the basis of a delegated law enacted in the autumn of 2012[10] to combat the proliferation of corrupt practices. This was in fact the so-called 'Anti-Corruption Law'.

This Legislative Decree presents a certain idea of transparency that breaks with the previous Italian tradition, according to which access was necessary to protect individuals from the power of public authorities. Access was considered a tool for citizens affected by the effects of some administrative decisions to be able to set up the appropriate means of defence (including jurisdictional) against administrative acts that infringed upon their prerogatives. On the contrary, the new type of access provided for by Legislative Decree no. 33/2013 responds to the need to guarantee knowledge of the reasons that inspire the actions of administrations. So, the new concept of transparency embodies the idea of collaboration with administrations, based on

* Article submitted to double blind peer review.

[1] A.G. Orofino, *La trasparenza oltre la crisi. Accesso, informatizzazione e controllo civico*, Bari, Cacucci, 2020.

[2] J. Valero Torrijos and M. Fernández Salmerón (eds.), *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*, Cizur Menor, Aranzadi, 2014; I.M. Delgado (ed.), *Transparencia y acceso a la información pública de la teoría a la práctica*, Madrid, Iustel, 2019; E. Guichot and C. Barrero Rodriguez, *El derecho de acceso a la información pública*, Valencia, Tirant lo Blanc, 2020.

[3] G.J. Guglielmi and É. Zoller (eds.), *Transparence, démocratie et gouvernance citoyenne*, Paris, Editions Panthéon-Assas, 2014.

[4] J. von Luche and K. Gollasch, *Open Government. Offenes Regierungs- und Verwaltungshandeln – Leitbilder, Ziele und Methoden*, Cham, Springer, 2022, 25. *Adde* F. Schoch and M. Kloepfer, *Informationsfreiheitsgesetz (IFG-ProfE): Entwurf eines Informationsfreiheitsgesetzes für die Bundesrepublik Deutschland*, Berlin, Duncker & Humblot, 2002.

[5] P. Birkinshaw, *Freedom of Information. The Law, the Practice and the Ideal*, 4th ed., Cambridge, Cambridge University Press, 2010.

[6] D.E. Pozen and M. Schudson, *Troubling Transparency. The History and Future of Freedom of Information*, New York, NY, Columbia University Press, 2018.

[7] J.M. Ackerman and I.E. Sandoval-Ballesteros, *The Global Explosion of Freedom of Information Laws*, in *Administrative Law Review*, vol. 58, 2006, 85.

[8] Legislative decree no. 33 of 14 March 2013.

[9] Law no. 15 of 4 March 2009 and legislative decree no. 150 of 27 October 2009.

[10] Law no. 190 of 6 November 2012.

participatory and administrative democracy.[11]

The previous Italian law on administrative access[12] expressly prohibited general requests aimed at monitoring the entire work of public bodies.[13] By contrast, the new legislative framework establishes a general principle of transparency. It specifies that this principle entails freedom of access to data, information and documents held by public administrations. This form of transparency aims to protect the rights of citizens but also to promote the participation of interested parties in administrative activity. So, it encourages widespread forms of control over the exercise of institutional functions and the use of public resources.[14]

2. *Administrative Transparency in the Age of Mistrust*

Legislative Decree no. 33/2013 has profoundly changed the meaning of transparency in Italy.[15] This form of transparency meets various objectives in accordance with what is expressly stated in the texts of the legislative decree. In particular, it is supposed to contribute to the implementation of various principles. We are talking about democratic and constitutional principles of equality, impartiality, responsibility, effectiveness and efficiency in the use of public resources, and the principles of integrity and loyalty in the service of the nation.

It is also a condition for guaranteeing individual and collective freedoms, as well as civil, political and social rights. Finally, transparency integrates the right to good administration and contributes to the achievement of an open administration at the service of individuals. Consequently, the new transparency provisions apply not only to those who suffer an injury deriving from the adoption of administrative acts. On the contrary, they apply to all citizens who are understood as holders of the sovereignty that the Constitution recognises to every citizen. Transparency thereby becomes a tool through which citizens can confront and communicate with administrations. The need for this new form of transparency is motivated by a deep mistrust of institutions[16] which is exacerbated by the difficulties faced by citizens as a result of the economic and social crisis that characterises the current period.[17]

In Italy, as well as in other countries, the enactment of laws providing measures to increase transparency has been justified also by the revelation of scandals involving important political figures. Parliaments have felt the need to enact certain rules in response to these scandals.[18] They have played into the hands of populists[19] and fuelled 'anti-political' feelings which have ultimately undermined the democratic legitimacy of institutions.

In an ever-increasingly divided and deconstructed society,[20] trust based on consensus and credibility of administrations and their representatives has been replaced by a new form of trust based on the possibility of direct control and verification. All this can be interpreted as a sign of the new weakness of institutions.[21]

3. *Open Data as an Instrument of Transparency*

In the same way that anti-politics has used the Internet as a means of expressing dissent, public bodies have also had to resort to online communication channels to strengthen

[11] J.-B. Auby, *Remarques préliminaires sur la démocratie administrative,* in *Revue française d'administration publique*, 2011, 137; J. Chevallier, *De l'administration démocratique à la démocratie administrative*, in *Revue française d'administration publique*, 2011, 217.

[12] See articles 22 et ff. of law no. 241 of 8 August 1990.

[13] A. Bonomo, *Informazione e pubbliche amministrazioni. Dall'accesso ai documenti alla disponibilità delle informazioni*, Bari, Cacucci, 2012.

[14] See art. 1 of legislative decree no. 33/2013.

[15] On the existence of different variations of the principle of transparency, see R. Feik, *Zugang zu EU-Dokumenten. Demokratie durch Transparenz*, Vien-Graz, Neuer Wiss, 2002, 13.

[16] P. Rosanvallon, *La contre-démocratie. La politique à l'âge de la défiance*, Paris, Seuil, 2006.

[17] A.G. Orofino, *La trasparenza oltre la crisi*. *Accesso, informatizzazione e controllo civico*, 13.

[18] A.G. Orofino, *Profili giuridici della trasparenza amministrativa*, Bari, Cacucci, 2013, 97. See also B. Nabli, *Fondements de la « moralisation-juridicisation » de la vie politique*, in *Pouvoirs*, no. 154, 2015, 149: 'À la suite de l'« affaire Cahuzac », le président François Hollande en a appelé à un « choc de moralisation » qui s'est traduit juridiquement par l'adoption des lois organique et ordinaire du 11 octobre 2013 relatives à la transparence de la vie publique'.

[19] P. Rosanvallon, *Le Siècle du populisme. Histoire, théorie, critique*, Paris, Seuil, 2020.

[20] J. Chevallier, *L'État post-moderne*, IV ed., Paris, Lextenso, 2017, 91.

[21] J. Bröhmer, *Transparenz als Verfassungsprinzip Grundsatz Und Europäische Union*, Mohr Siebeck, 2004, 8: 'Das Auf kommen des Transparenzthemas in der öffentlichen Diskussion hat auch zu tun mit einer zu beobachtenden Veränderung der Rolle des – westeuropäische – Staates. Der Staat verliert zunehmend seine Rolle als Prinzipale politische Gestaltungsinstanz'.

political consensus and, consequently, the legitimacy of public authorities. It is for these reasons that the recent Italian regulations on transparency provide for the online dissemination of data, documents and information inherent to the exercise of public functions.

In particular, Legislative Decree no. 33/2013 created what is known as 'accesso civico' (civic access). As mentioned above, it gives the possibility for citizens to access certain documents, data or information held by administrations. This is possible even when the request is not motivated by a particular interest or reason.

In some cases, access requires a request from citizens. In other cases, and for certain information mentioned by the law, dissemination is by publication on the Internet. In this case there is no need for any requests from citizens.

Under the terms of legislative decree no. 33/2013, administrations have the duty to publish a wide range of data and information. These relate to contracts signed by public authorities, organisation of offices, information on town planning and environmental issues, etc.

This is a large amount of data. When it is subject to mandatory publication it must be published in open format[22] and be reusable.[23] The reuse can be made without any restrictions other than the obligation to cite the source and respect the integrity[24] of the information. All data must be processed in a way that it can be indexed and tracked by search engines.[25]

The Digital Administration Code also deals with open data.[26] It defines open data as being that which is: (a) available under licences or normative provisions allowing use by any person, even in a disaggregated format, (b) is accessible in open formats and suitable for automatic processing by computer programs, (c) and made available via computer networks free of charge or at very low cost. An entire section is devoted to public-administration data (Chapter V, Section I). It establishes the obligation to manage data held by administrations in such a way as to allow re-use by different administrations where use is necessary for the performance of certain institutional tasks. This must be done within the limits set for the protection of privacy by the GDPR or by other regulations. This provision therefore implies that all data published by all public authorities is considered to be open data unless expressly exempted.[27]

Italian legislation therefore seems to express the idea that open data is a tool that helps to increase the transparency of administrations as already expressed in the Open Data Charter signed in 2013 by the G8 leaders.[28]

4. *Open Data as a Tool for Good Administration*

Open data certainly contributes to the creation of participative administrations. Thanks to a deeper knowledge of the facts on which the institutions are called upon to decide, it can also be used as a tool to guarantee greater efficiency in the performance of activities. This perspective is clearly affirmed in recent EU acts dealing with the re-use of public sector information.[29]

The importance of the cognitive activity carried out by the administrations has been emphasised on several occasions by legal scholars, including those that analysed this topic in the first decades after enacting the Italian Constitution.[30] The use of powerful

[22] Art. 7 of legislative decree no. 33/2013.
[23] Legislative decree no. 36 of 24 January 2006.
[24] Art. 7 of legislative decree no. 33/2013.
[25] Art. 7 *bis* of legislative decree no. 33/2013.
[26] Art. 1, lett. i), of legislative decree no. 82 of 7 March 2005.
[27] Art. 52 of legislative decree no. 82/2005.
[28] The Open Data Charter states that 'open data can increase transparency about what government and businesses are doing. Open data also increase awareness about how countries' natural resources are used, how extractives revenues are spent, and how land is transacted and managed. All of which promotes accountability and good governance, enhances public debate, and helps to combat corruption. Transparent data on G8 development assistance are also essential for accountability' (the document is available at https://opendatacharter.net).
[29] See in particular the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 February 2022 COM(2020) 66 final on a European Data Strategy. See also Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. Further information on the European Data Strategy can be found on the EU website at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#data-governance.
[30] V. Ottaviano, *La comunicazione degli atti amministrativi*, Milan, Giuffré, 1953; F. Levi, *L'attività conoscitiva della pubblica amministrazione*, Turin, Giappi-

knowledge tools makes this cognitive activity more effective. Such tools have obvious advantages in terms of the quality of the work conducted by administrations and also enhances the transparency of the activities carried out. The principle of transparency is in fact applicable to rules aimed at guaranteeing adequate investigation and assessment of the facts to enable conscious and careful decision to be made.[31]

This is why Italian legislation provides for the creation of various databases, to facilitate the sharing of information between administrations. The most important of these is probably the 'Piattaforma digitale nazionale dati' (National Digital Data Platform). It is intended to serve and facilitate the exchange of public information by all the institutions that need to access them in order to carry out their tasks.

There are also plans to create sectoral databases, such as the national register of people assisted by the national health service.[32] This will make it possible to control spending in the health sector, speed up the process of automating the management of health needs and improve health-protection services. For evidence of the efficiency of these tools, suffice it to think of the number of models and algorithmic predictions that have been used during the health emergency to forecast trends in pandemic curves. Other sectoral databases include the National Public Procurement Database[33] and the Education Database.[34]

The availability of information within shared platforms requires the identification of technical solutions that guarantee data accessibility, protection, integrity and confidentiality, as well as the operational continuity of systems and infrastructures. To this end, the Agenzia per l'Italia Digitale (Agid) should play a particularly important role both by adopting appropriate guidelines to regulate the production and exchange of public data and by supervision.[35]

5. *Some Concluding Remarks*

The discussion so far clearly shows that the subject of transparency is linked to that of open data from two perspectives. First, from the viewpoint of citizens for whom transparency becomes an instrument of participation and civic control. This is sometimes exercised directly and sometimes exercised through operators such as journalists and associations that pursue statutory objectives of civic protection in certain sectors. Secondly, it must be considered that it is a fundamental tool for the administrations to be able to process data both manually and digitally. It enables them to make better informed and more careful decisions and, consequently, better verifiable ones.

The administrative environment is often characterised by the isolation of administrative bodies which work without dialogue or exchange of experience. So, the lack of information sharing has often been at the root of mistakes made by institutions as well as episodes of maladministration. The exchange of useful data to improve the performance of public functions can only benefit the administrations themselves.

chelli, 1967.

[31] A. Police, *Trasparenza e formazione graduale delle decisioni amministrative*, in *Diritto amministrativo*, 1996, 229.

[32] Art. 62 *ter* of legislative decree no. 82/2005.

[33] Art. 62 *bis* of legislative decree no. 82/2005. It may be appropriate to point out that also in France, Article L. 3131-2 du *Code de la commande publique* states that the concessionaire of a public service must provide the contracting authority, in electronic form and in a freely reusable open format, the data and databases collected and produced during the course of performance of the contract. See T. Bassi, *Les données collectées par le concessionnaire de service public*, in *Aida*, 2019, no. 9, 496.

[34] Art. 62 *quater* of legislative decree no. 82/2005.

[35] For an indication of the various initiatives taken by Agid in this area, see the page: www.dati.gov.it/fare-open-data/Strumenti-per-gli-Open-Data.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 55-61
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 0.53136/9791221807981 07

*The Regulation (EU) 2018/1807 on a Framework for the Free Flow of non-Personal Data in the European Union and its Implementation by Public Administrations**

Joel A. Alves
(Researcher at the Research Centre for Justice and Governance of the University of Minho)

ABSTRACT This article has a two-fold objective: (i) firstly, it aims to present the main features of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union; (ii) secondly, it seeks to reflect on how those may affect public administrations – one of the most relevant players in the European data economy.

1. *Introduction*

Back in 2014, the European Commission expressed its belief that a thriving data-driven economy could bring huge benefits for people, business, and public administrations.[1] Since then, that conviction has not been weakened, but rather reinforced. Nevertheless, one thing came clear: for this to happen, any Member-State action affecting data storage or processing should be guided by a *principle of free movement of data within the internal market*.[2]

Building on these premises, the European Parliament and the Council have adopted the Regulation (EU) 2018/1807,[3] which aims to ensure the *free flow of data other than personal data within the European Union*, by laying down rules relating to *data-localisation requirements*, the *availability of data to competent authorities* and the *porting of data for professional users*.[4] The idea was to fill the gaps in the existing legal framework,[5] providing for a coherent set of rules that cater for the free movement of different types of data within the Union's borders.[6] This is because the General Data Protection Regulation already prohibited restrictions on the free flow of data within the European Union *on grounds connected with the protection of personal data*.[7] However, limitations based on *other reasons* – e.g. restrictions provided for under tax or accounting laws for purposes of regulatory control[8] – were not covered by such legal instrument.[9] Furthermore, *data other than*

* Article submitted to double-blind peer review.
This article was written with a support of a PhD Research scholarship from the Portuguese national funding agency for science, research and technology (fellowship no. 2022.13673.BD).

[1] See European Commission, COM(2014) 442 final, *Towards a thriving data-driven economy*, 2 July 2014, 12.

[2] See European Commission, COM(2017) 9 final, *Building a European Data Economy*, 10 January 2017, 7.

[3] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, hereinafter, referred to as "Regulation (EU) 2018/1807" or simply "the Regulation".

[4] See article 1 of the Regulation.

[5] See P.J. Muñoz, *Algunas reflexiones acerca de la propuesta de Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*, in F. Galindo (ed.), *¿Como poner en práctica el gobierno abierto?*, Madrid, Editorial Reus, 2019, 52 f.

[6] See recital 10 of the Regulation. In the same vein, see European Commission, COM(2019) 250 final, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, 29 May 2019, 2.

[7] See article 1(3) of the General Data Protection Regulation, where the following is stated: "the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data". For further developments, see J.L.P. Mañas, *Objecto del Reglamento*, in J.L.P. Mañas, M.A. Caro and M.R. Gayo (eds.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Madrid, Editorial Reus, 2016, 51 f. and 55 ff.

[8] An example of such a restriction would be a national law that requires payroll accounts to be located in a particular Member State, for reasons connected to regulatory control, e.g., by the national tax authority. See European Commission, COM(2019) 250 final, 13.

[9] See European Commission, COM(2017) 228 final, "A

personal data were equally left outside of its material scope.[10]

In this vein, this article has a two-fold objective: (i) firstly, it aims to present the main features of this (still) recent piece of legislation: (ii) secondly, it seeks to reflect on how those may affect public administrations – one of the most relevant players in the data economy.[11]

2. *Main features*

2.1. *The principle of free flow of non-personal data across borders*

Aligned with the Commission communication "Building a European Data Economy",[12] Regulation (EU) 2018/1807 openly recognizes that enabling data to flow freely across borders is almost a precondition to achieve data-driven growth and innovation.[13] Accordingly, the mentioned legal instrument proposes to establish, with regard to *non-personal data*, the *principle of free movement within the European Union* similar to the one provided for, under the General Data Protection Regulation, *vis-à-vis personal data.*[14]

Conversely to the latter, the restrictions on the free flow of data that the Regulation (EU) 2018/1807 intends to tackle do not, however, originate from the existence of different national standards, between the Union's Member States, concerning the protection of the rights and freedoms of natural persons.[15] They rather arise from certain "requirements in the laws of Member States to locate data in a specific geographical area or territory for the purpose of data processing".[16] But also, from "other rules or administrative practices [that] have an equivalent effect by imposing specific requirements which make it more difficult to process data outside a specific geographical area or territory within the Union".[17]

In the light of the above, article 4(1) of the Regulation sets out that "data localisation requirements[18] shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality". This means that, as a general rule, Member States should not be able to force organisations to locate the storage or processing of data within their borders.[19] Restrictions will only be justified for reasons of public security.[20] And, even in that case,

Connected Digital Single Market for All", 10 May 2017, 10.

[10] See article 2(1) of the General Data Protection Regulation, read in conjunction with article 4(1) thereof. For further developments, see A. von dem Bussche and P. Voigt, *The EU General Data Protection Regulation (GDPR): a practical guide*, Cham, Springer, 2017, 9 ff.

[11] This idea is supported by recital 8 of Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public-sector information, where it reads: "The public sector in Member States collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, political, economic, legal, geographical, environmental, meteorological, seismic, touristic, business, patent-related and educational areas. Documents produced by public sector bodies of the executive, legislature or judiciary constitute a vast, diverse and valuable pool of resources that can benefit society". Similarly, recital 9 states: "Public sector information represents an extraordinary source of data that can contribute to improving the internal market and to the development of new applications for consumers and legal entities".

[12] See European Commission, COM(2017) 9 final, 7.

[13] See recital 13 of the Regulation.

[14] See recital 10 of the Regulation.

[15] See P.A.M. Asensio, *Servicios de almacenamiento y tratamiento de datos: el Reglamento (EU) 2018/1807 sobre libre circulación de datos no personales*, in *La Ley Unión Europea*, n. 66, 2019, 4.

[16] See recital 4 of the Regulation.

[17] Idem.

[18] Pursuant to article 4(1) of the Regulation a "data-localisation requirement" should be understood as "any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State". This means that, for the purposes of the Regulation, "data-localisation requirements" can take various forms: they may be set out in laws, in administrative regulations and provisions or even result from general and consistent administrative practices. Also, they may consist either in direct or indirect restrictive measures. Examples of the formers would be an obligation to store data in a specific geographic location (e.g. servers must be located in a particular Member State) or an obligation to comply with unique national technical requirements (e.g. data must use specific national formats). Regarding the latter, they may include requirements to use technological facilities that are certified or approved within a specific Member State or other requirements that have the effect of making it more difficult to process data outside of a specific geographic area or territory within the European Union. For further developments, see European Commission, COM(2019) 250 final, 11 f.

[19] See European Commission, *State of the Union 2017: A framework for the free flow of non-personal data in the EU*, 19 September 2017.

[20] See recital 18 of the Regulation. In any case, recital 19 recalls that the concept of "public security", as defined by Union law and as interpreted by the Court of Justice, presupposes "the existence of a genuine and

they (i) must be suitable for attaining the objectives pursued, and (ii) must not got beyond what is necessary to attain these objectives.[21]

It follows that, after a transitional period of 24 months from the data of application of the Regulation – which has already lapsed[22] – any existing data-localisation requirements that are not in compliance with the aforesaid conditions shall be repealed.[23] Besides that – "in order to ensure the effective application of the principle of free flow of non-personal data across borders, and to prevent the emergence of new barriers to the smooth functioning of the internal market"[24] – Member States are also required to communicate to the Commission any draft act[25] which introduces new data-localisation requirements or make changes to existing data-localisation requirements in conformity with the procedures set out in articles 5, 6 and 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.[26]

Furthermore – and so as to promote transparency *vis-à-vis* natural and legal persons, including *service providers* and *users of data-processing services*[27] – the Regulation obliges Members States to make the details of any data-localisation requirements applicable in their territory publicly available via a national online single information point, which shall be kept up-to-date. Or, alternatively, to provide up-to-date details on such requirements to a central information point established under another Union act.[28] In any case, the same legal instrument sets out that Member States should notify to the Commission the address of such single information points. Subsequently, for the convenience of businesses and to provide for their easy access to relevant information across the Union, the Commission shall publish the links to these information points on its website (i.e., the Your Europe portal[29]), along with a regularly-updated and consolidated list of all data-localisation requirements, including summary-information on those requirements.[30]

2.2. *The principle of data availability for regulatory control*

Notwithstanding the foregoing, the legislator seemed to be conscious that data-localisation requirements frequently stemmed from a lack of trust in cross-border data processing, founded on the presumed unavailability of data for regulatory purposes.[31] This is because, as previously pointed out by the European Commission, a number of Member States apparently believed that data would be more easily accessible for their national competent authorities if they were stored or processed locally[32] – even if, in practice, data-localisation restrictions rarely proved to be a measure suitable to achieve that objective.[33]

In this vein, the Regulation seeks to overcome this problem, by establishing a new cooperation mechanism, aiming to ensure that competent authorities stay able to exercise any rights they have to access data that are being processed in other Member States.[34] The idea is simple: the prohibition of data-location restrictions shall not affect the powers of

sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interest". So that, to make use of that exception, Member States must give evidence that the data localisation requirements they want to put in place are justified on one of such grounds.

[21] See recital 18 of the Regulation.

[22] As follows from article 4(3) of the Regulation, the referred transitional period ended on 30 May 2021.

[23] See article 4(3) of the Regulation, read in conjunction with recital 21 thereof.

[24] See recital 20 of the Regulation.

[25] For the purposes of the Regulation, "draft act" should be understood as any "text drafted for the purpose of being enacted as a law, regulation or administrative provision of a general nature, the text being at the stage of preparation at which substantive amendments can still be made". See article (2)(3) of the Regulation.

[26] See article 4(2) of the Regulation. In our view also existing data-localisation requirements that, despite being considered as legitimate, were not communicated to the Commission, for the purposes and in accordance with article 4(3) of the Regulation, by 30 May 2021, should be covered by subject to this requirement.

[27] See recital 23 of the Regulation.

[28] See article 4(4) of the Regulation.

[29] See European Commission, COM(2019) 250 final, 13. The said portal is available at https://europa.eu/youreurope/index.htm.

[30] See article 4(5) of the Regulation, read in conjunction with recital 23 thereof.

[31] See recital 24 of the Regulation.

[32] See European Commission, COM(2017) 9 final, 6.

[33] Idem, ibidem.

[34] See European Commission, COM(2019) 250 final, 3.

competent authorities[35] to request or obtain access to data for the performance of their official duties in accordance with Union or national law.[36] So that, such authorities cannot be refused access to data on the basis that the data are processed in another Member State.[37]

As a result, where a natural or legal person is subject to an obligation to provide data and fails to comply with that obligation, the competent authority may request assistance from a competent authority in another Member State, by submitting a fully-justified request to the latter's designated single point of contact.[38] Nevertheless, it will only be able to make use of this power in the absence of specific cooperation instruments in Union law or under international agreements.[39] Still, whereas a request for assistance entails obtaining access to any premises of natural or legal person, including to any data-processing equipment and means, by the requested authority, such access must be in accordance with Union law or national procedural law, including any requirement to obtain prior judicial authorisation.[40]

At any rate, it is stressed that the Regulation should not allow users to attempt to evade the application of national law.[41] This is why article 5(4) of such legal instrument stipulates that "Member States may impose effective, proportionate and dissuasive penalties for failure to comply with an obligation to provide data, in accordance with Union and national law". Moreover, the same provision equally states that, in urgent cases, where users abuse their right, Member States should also be able to impose strictly proportionate interim measures, such as requiring the (temporary) re-localisation of the data.[42]

2.3. *Porting data and switching between data-processing services*

While removing data-localisation restrictions was considered the most important factor to unleash the full potential of the data economy in the European Union,[43] recital 2 of the Regulation still notes that there were other obstacles to data mobility and to the internal market that demanded attention – namely, *vendor lock-in practices in the private sector*, i.e., practices hindering users of data-processing services from switching between service providers, by «locking» their data in the provider's system (e.g. due to a specific data format or contractual arrangements) and making it unable to be transferred outside of that.[44]

On this point, though, the said legal instrument does not provide for specific obligations.[45] Instead, it limits to stimulate industry self-regulation,[46] by establishing that the Commission shall encourage the development of codes of conduct at Union level, covering, *inter alia*, the following aspects: (i) *best practices* for facilitating the switching of service providers and the porting of data in a structured, commonly-used and machine-readable format including open-standard formats where required or requested by the service provider receiving the data;[47] (ii) *minimum information requirements* to ensure that professional users are provided,

[35] For the purposes of the Regulation, "competent authority" should be understood as any "authority of a Member State or any other entity authorized by national law to perform a public function or to exercise official authority, that has the power to obtain access to data processed by a natural or legal person for the performance of its official duties, as provided for by Union or national law. See article 3(6) of the Regulation.

[36] See article 5(1) of the Regulation, read in conjunction with recital 24 thereof.

[37] See article 5(1) of the Regulation, read in conjunction with recital 24 thereof.

[38] See article 5(2) of the Regulation, read in conjunction with article 7 and recital 32 thereof.

[39] See recital 26 of the Regulation. Pursuant to that provision, examples of such specific cooperation instruments would be, "in the area of police cooperation, criminal or civil justice or in administrative matters respectively, the Council Framework Decision 2006/960/JHA, Directive 2014/41/EU of the European Parliament and of the Council, the Convention on Cybercrime of the Council of Europe, Council Regulation (EC) No. 1206/2001, Council Directive 2006/112/EC, and Council Regulation (EU) No 904/2010".

[40] See article 5(3) of the Regulation, read in conjunction with recital 27 thereof.

[41] See recital 28 of the Regulation.

[42] See article 5(4) of the Regulation. Nonetheless – and according to this provision – if the re-localisation of data is imposed for a duration that is longer than 180 days following re-localisation, it should be communicated to the Commission, within that 180-day period, for the examination of their compatibility with Union Law.

[43] See European Commission, *State of the Union 2017: A framework for the free flow of non-personal data in the EU*.

[44] See European Commission, COM(2019) 250 final, 16 f.

[45] See P.A.M. Asensio, *Servicios de almacenamiento y tratamiento de datos: el Reglamento (EU) 2018/1807 sobre libre circulación de datos no personales*, 7.

[46] Idem, ibidem.

[47] See article 6(1)(a) of the Regulation.

before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply in case professional users want to switch to another service provider or port data back to their own IT systems;[48] (iii) *approaches to certification schemes* that facilitate the comparison of data-processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services;[49] and (iv) *communication roadmaps* taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.[50] Also, the Regulation requires the Commission to ensure that such codes be developed in close cooperation with all relevant stakeholders, including associations of SMEs and start-ups, users and cloud service providers.[51]

3. *Impact on public administrations*

3.1. *General obligations*

That said, Regulation (EU) 2018/1807 leaves no room for doubts in what regards the applicability of its provisions to public administrations. In fact, recital 13 thereof is unambiguous: "public authorities and bodies governed by public law should be covered by [the scope of] this Regulation".[52] This is confirmed by article 2(1) of the same legal instrument, where the following is stated: "the Regulation applies to the processing of electronic data other than personal data in the Union, which is: (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the European Union; or; (b) *carried out by a* natural or *legal person* residing or *having an establishment in the Union for its own needs*" (italics added).

To put it simply: pursuant to the referred legal provision, Regulation (EU) 2018/1807 should apply to *service providers*, who provide data-processing services to users residing or having an establishment in the European Union (including those who provide data-processing services in the Union without an establishment in that legal area).[53] But also, to *any natural or legal person residing or having an establishment in the European Union who processes data for its own needs.* Consequently, the decision of whether public administrations should, or should not, be subject to the obligations laid down in such legal instrument, in a particular case, would be exclusively dependent on the interpretation of two key terms: the notion of "processing";[54] and the notion of "data other than personal data".[55]

At any rate, article 2(2) of the Regulation makes clear that those obligations shall also apply to the processing of *mixed data sets*[56] –

[48] See article 6(1)(b) of the Regulation.
[49] See article 6(1)(c) of the Regulation. Pursuant this provision, "such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management".
[50] See article 6(1)(d) of the Regulation.
[51] See article 6(2) of the Regulation.
[52] This solution is consistent with the General Data Protection Regulation, who also applies both to public and private entities. For further developments, see J.A. Alves, *The General Data Protection Regulation and its application to the public sector*, in *PoLaR – Portuguese Law Review*, vol. 4, n. 2, 2020, 179 ff.
[53] See recital 15 of the Regulation.
[54] Pursuant to article 3(2) of the Regulation, the concept of "processing" should be understood as "any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". This provision closely follows the concept of processing of personal data enshrined in article 4(2) of the General Data Protection Regulation, stating: "processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".
[55] As already explained by the European Commission, this concept is defined by opposition (*a contrario)* to the notion of personal data, provided for under article 4(1) of the General Data Protection Regulation. See article 3(1) of the Regulation. For further developments, see European Commission, COM(2019) 250 final, 4 ff. On the concept of "personal data" see also Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 6 ff.
[56] Nonetheless – and according to the aforementioned provision – those obligations will only apply to the *non-personal data* part of the data set. The remaining part – i.e., the *personal-data* part – shall be subject to the relevant rules and principles provided for under the General Data Protection Regulation. Furthermore, if the *non-personal data* part and the *personal-data part* are "inextricably linked", the General Data Protection Regulation should fully apply to the whole mixed set, even if personal data represent only a small part of the data set. For further developments, see European Commission, COM(2019) 250 final, 9.

i.e., data sets composed of both *personal* and *non-personal data*[57], which represent the majority of the data sets used in the data economy.[58]

Despite the above, it should however be mentioned that, as Directive 2014/24/EU,[59] Regulation (EU) 2018/1807 is without prejudice to laws, regulations, and administrative provisions which relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as the laws, regulations and administrative provisions of Member States that provide for the implementation of those powers and responsibilities.[60] Therefore, while encouraging public administrations to consider economic and other benefits of outsourcing to external service providers, nothing in this legal instrument obliges them to contract out or externalise the provision of services that they wish to provide themselves or to organise by means other than public contracts.[61] Moreover, the Regulation also points out that it should not affect data processing in so far as it is carried out as part of activities which fall outside the scope of Union law (e.g., activities related to national security).[62]

3.2. *Indirect benefits*

Nevertheless, one must not forget that public administrations will often act as "competent authorities", in the meaning of article 3(6) of the Regulation.[63] Thus, irrespective of the referred obligations, they will still be (positively) impacted by such legal instrument when requesting or obtaining access to data for the purposes and in accordance with article 5 thereof.

Furthermore, public administrations might also be "users" of data-processing services (e.g. when outsourcing the storage of non-personal data on cloud-services providers).[64] So, like business and consumers, they are expected to take advantage from the removal of unjustified data-localisation requirements, which hampered the freedom to provide services and the freedom of establishment within the Digital Single Market.[65] After all, this will presumably result in huge benefits, ranging from an increased freedom of choice regarding data-driven service providers to access to cheaper and more innovative solutions.[66]

Finally, as "professional users",[67] public administrations stand to benefit from the ability "to make informed choices and to easily compare the individual components of various data-processing services offered in the internal market, including in respect of the contractual terms and conditions of porting data upon the termination of a contract",[68] provided for future self-regulatory codes of conduct, adopted under article 6 of the Regulation.[69]

4. *Final remarks*

Despite all the criticism it has been attracted,[70] Regulation (EU) 2018/1807 constitutes an important step[71] to enable the European Union to become "the most attractive, most secure and most dynamic data-agile economy in the world".[72]

[57] See European Commission, COM(2019) 250 final, cit., 8.
[58] Idem, ibidem.
[59] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.
[60] See article 2(3) of the Regulation, read in conjunction with recital 14 thereof.
[61] See recital 14 of the Regulation.
[62] See article 2(3) of the Regulation, read in conjunction with recital 12 thereof.
[63] See P.J. Muñoz, *Algunas reflexiones acerca de la propuesta de Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*, 57 ff.
[64] Pursuant to article 2(3) of the Regulation "user" means "a natural or legal person, *including a public authority or body governed by public law*, using or requesting a data processing service" (emphasis added).
[65] See recital 18 of the Regulation. In the same vein, see European Commission, COM(2017) 9 final, 3.
[66] See recital 13 of the Regulation.
[67] Article 2(8) of the Regulation defines "professional user" as "a natural or legal person, *including a public authority or a body governed by public law,* using or requesting a data processing service for purposes related to its trade, business, craft, profession or task" (emphasis added).
[68] See recital 30 of the Regulation.
[69] See, in particular, article 6(1)(b) of the Regulation.
[70] While referring to the proposal of the European Commission on which the Regulation is founded, see, by way of example, D. Broy, *The European Commission's Proposal for a Framework for the Free Flow of Non-Personal Data in the EU*, in *European Data Protection Law Review*, vol. 3, n. 3, 2017, 383.
[71] In a similar vein, see P.J. Muñoz, *Algunas reflexiones acerca de la propuesta de Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*, 51f and 61.
[72] This ambition has been recently restated by the European Commission, under its communication

Given the large amounts of data that public administrations handle, it is therefore of the utmost importance that they lead by example,[73] by complying fully with their obligations under such legal instrument – including those arising from the *principle of free flow of non-personal data across borders*[74] and the *principle of availability of data for regulatory control*[75].

Nonetheless, the Regulation should not be seen merely as a legal burden, but also as a chance: a chance for public administrations to make the most of digital and data technologies.

entitled *A European strategy for data*. See European Commission, COM(2020) 66 final, *A European strategy for data*, 19 February 2020, 25.

[73] See recital 13 of the Regulation.

[74] See article 4(1) of the Regulation.

[75] See article 5(1) of the Regulation.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 63-115
ISSN 2724-5969 – ISBN 979-12-218-0798-1 - DOI 10.53136/9791221807981 08

*La protezione dei dati personali nella pubblica amministrazione. L'esperienza italiana**

Sergio Niger
(Data Protection Officer at the University of Calabria, Professor of Security and Legal Issues of Computer Science at the Department of Mathematics and Informatics, University of Calabria)

ABSTRACT 25 May 2018, the Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) became fully operational. The GDPR obliges public administrations to adopt a series of appropriate technical and organizational measures to ensure that the processing of personal data takes place in compliance with the provisions of the GDPR. The most recent innovations introduced by the legislator in terms of transparency and publicity of administrative action, as well as the availability of documents, provide for various obligations for public entities to make the related information available. Mandatory disclosure must be balanced in compliance with the provisions of the GDPR.

1. *L'impatto del Regolamento UE 2016/679 sulle Amministrazioni Pubbliche*

Nel corso degli ultimi anni la pubblica amministrazione è stata investita da un poderoso processo di riforma, caratterizzato da rilevanti innovazioni normative che hanno imposto agli uffici pubblici una necessaria rivoluzione organizzativa e culturale, nonché un progressivo e faticoso adeguamento alle nuove prescrizioni.

Semplificazione amministrativa, trasparenza, prevenzione dei fenomeni di corruzione, processo di digitalizzazione, nuovo Codice dei contratti, queste sono solo alcune delle sfide con le quali gli uffici pubblici sono chiamati ogni giorno a confrontarsi.

Il processo di modernizzazione del settore pubblico in molti paesi "occidentali" è avvenuto in contemporanea con l'affermarsi delle nuove tecnologie ICT, che hanno generato importanti impatti sulla società, sulle relazioni tra individui e organizzazioni e all'interno delle stesse. In particolare, le ICT hanno contribuito a modificare in modo radicale l'accesso alle informazioni, così come i confini spazio-temporali tra individui e istituzioni pubbliche e private, modificando fabbisogni e abitudini dei cittadini. Nel soddisfare gli utenti, le ICT rispondono a tre importanti esigenze delle amministrazioni pubbliche nel processo di erogazione dei propri servizi: accessibilità, fruibilità, riduzione delle barriere spazio-temporali dei confini dell'amministrazione. Tutto ciò implica nuove modalità nella gestione delle nuove tecnologie e la tipologia di risposta deve essere univoca. È, pertanto, necessaria una forte riorganizzazione interna finalizzata all'eliminazione della frammentazione organizzativa e alla gestione condivisa ed integrata di informazioni relative ai servizi e alle richieste da parte degli utenti, i quali si aspettano risposte coerenti e in grado di soddisfare i propri bisogni.

Occorre, quindi, porsi nella logica del cambiamento sapendo che l'innovazione è cambiamento in pratica e che, pertanto, richiede una progettualità del percorso di trasformazione che non si esaurisce nella norma o nella decisione di innovare. A tal fine è necessario tener conto delle difficoltà, delle resistenze, con chiari progetti di gestione del cambiamento, con la definizione di precise responsabilità degli attori coinvolti, gli strumenti utilizzati, i percorsi da seguire in termini di competenze da sviluppare.

Le riforme amministrative degli ultimi anni hanno imposto alle amministrazioni pubbliche uno specifico dovere informativo, in quanto obbligano i soggetti pubblici a fornire informazioni su normative, attività e strutture amministrative, nonché sul funzionamento e l'erogazione dei servizi pubblici, a prescindere da un'esplicita richiesta proveniente dai cittadini.

Le più recenti novità introdotte dal legislatore in tema di trasparenza e pubblicità dell'azione amministrativa nonché di consultabilità degli atti prevedono in capo ai soggetti pubblici diversi obblighi di messa a disposizione delle relative informazioni.

* Article submitted to double-blind peer review.

Nel processo di trasformazione della pubblica amministrazione si inserisce (dal 25 maggio 2018) anche il Regolamento UE 2016/679 (*Regolamento Generale sulla protezione dei Dati*, d'ora in poi RGPD)[1], che nelle disposizioni che lo compongono riflette tutti i mutamenti avvenuti negli ultimi anni, dalla Direttiva 95/46/CE, in ambito tecnologico, economico, sociale, politico, antropologico. Con il RGPD l'Unione europea ha inteso rafforzare la tutela del diritto dei cittadini alla protezione dei dati personali, riflettendone la natura di diritto fondamentale dell'Unione stessa (art. 8 Carta dei diritti fondamentali dell'Unione e art. 16 del TFUE). Attraverso la previsione di un unico insieme di disposizioni direttamente applicabili negli ordinamenti giuridici degli Stati membri, l'U.E. vuole garantire la libera circolazione dei dati personali tra gli Stati membri e rafforzare la fiducia e la sicurezza dei consumatori, due elementi considerati indispensabili nell'ottica del nuovo mercato unico digitale[2].

Il RGPD segue l'impostazione della c.d. "direttiva madre" sulla protezione dei dati ma, facendo tesoro di vent'anni di legislazione dell'UE in materia e di giurisprudenza pertinente, chiarisce e modernizza le norme concernenti tale protezione e introduce alcuni elementi innovativi che rafforzano la tutela dei diritti delle persone e contemplano nuovi adempimenti, ma anche opportunità, per le amministrazioni pubbliche e per i soggetti privati, ossia: un quadro giuridico armonizzato che porta a un'applicazione uniforme delle norme a vantaggio del mercato unico digitale dell'Unione; parità di condizioni per tutte le imprese che operano sul mercato dell'Unione. Il RGPD impone alle imprese con sede al di fuori dell'UE di applicare le stesse norme vigenti per le imprese stabilite nell'UE quando trattano dati personali in relazione all'offerta di beni e servizi o al monitoraggio del comportamento dei cittadini nell'Unione. Le imprese che operano dall'esterno dell'UE e sono attive sul mercato unico devono, in determinate circostanze, nominare un rappresentante nell'UE al quale i cittadini e le autorità possano rivolgersi in aggiunta o in sostituzione dell'impresa con sede all'estero; i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita, che creano incentivi ad adottare sin dall'inizio soluzioni innovative in risposta ai problemi di protezione dei dati; diritti dei singoli rafforzati. Il regolamento introduce nuovi requisiti in materia di trasparenza e diritti rafforzati in materia di informazione, accesso e cancellazione; il silenzio o l'inattività non saranno più considerati valide espressioni di consenso, in quanto è richiesto un atto positivo inequivocabile per esprimerlo; è garantita la protezione dei minori online; maggiore controllo dei singoli sui propri dati personali (ad es. il diritto alla portabilità dei dati); maggiore protezione contro la violazione dei dati (c.d. *data breach*); il RGPD conferisce a tutte le autorità di protezione dei dati il potere di infliggere sanzioni pecuniarie ai titolari del trattamento e ai responsabili del trattamento; maggiore flessibilità per i titolari del trattamento e i responsabili del trattamento che trattano dati personali, grazie a disposizioni univoche in materia di responsabilità (principio di responsabilizzazione). Il regolamento si discosta da un sistema di notifica in favore del principio di responsabilizzazione, attuato tramite obblighi modulabili in funzione del rischio (per esempio l'obbligo di designare un responsabile della protezione dei dati o l'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati). Al fine di agevolare la valutazione del rischio prima di procedere al trattamento, è stato introdotto un nuovo strumento: la valutazione d'impatto sulla protezione dei dati. Quest'ultima, come

[1] L. Califano e C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2018; G. Comandè e G. Malgieri (a cura di), *Manuale per il trattamento dei dati personali: le opportunità e le sfide del nuovo Regolamento europeo sulla Privacy*, Roma, Il Sole 24 Ore, 2018; V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019; G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017; F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018; R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè, 2021; F. Pizzetti (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021.

[2] Cfr. Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018*, del 24 gennaio 2018.

vedremo in seguito, è richiesta ogniqualvolta il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche; maggiore chiarezza riguardo agli obblighi dei responsabili del trattamento e alla responsabilità dei titolari del trattamento quando selezionano un responsabile del trattamento; un sistema di *governance* moderno per garantire un'applicazione più coerente ed efficace delle norme. Il sistema prevede poteri armonizzati per le autorità di protezione dei dati, anche per quanto riguarda le sanzioni pecuniarie, e nuovi meccanismi di cooperazione in rete tra tali autorità; la protezione dei dati personali garantita dal regolamento segue i dati al di fuori dell'UE assicurando un livello elevato di protezione. In conformità con quanto prescritto dal RGPD, gli Stati membri devono adottare le misure necessarie per la rispettiva legislazione abrogando e modificando le norme esistenti, offrendo a questi la possibilità di precisare ulteriormente l'applicazione delle norme in materia di protezione dei dati in ambiti specifici, ossia: settore pubblico (art. 6, par. 2), rapporti di lavoro e sicurezza sociale (art. 88 e art. 9, par. 2, lett. *b*), medicina preventiva e medicina del lavoro, sanità pubblica (art. 9, par. 2, lett. *h* e *i*), fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici (art. 9, par. 2, lett. *j*), numero di identificazione nazionale (art. 87), accesso del pubblico ai documenti ufficiali (art. 86) e obblighi di segretezza (art. 90). Infine, per quanto concerne il trattamento di dati genetici, dati biometrici o dati relativi alla salute, il RGPD consente agli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni (art. 9, par. 4). "Le azioni degli Stati membri in questo contesto sono delimitate da due elementi:1. l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea ("Carta"), nel senso che qualsiasi legge nazionale volta a precisare le norme del regolamento deve soddisfare le condizioni previste dall'articolo 8 della Carta (e dal regolamento, che si fonda su detto articolo), e 2. l'articolo 16, paragrafo 2, del TFUE, in base al quale la legislazione nazionale non può interferire con la libera circolazione dei dati personali all'interno dell'Unione"[3].

[3] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Maggiore protezione, nuove opportunità*, 9.

Il RGPD impone alle amministrazioni pubbliche nuovi adempimenti, che non siano, però, solo di carattere formalistico e burocratico, secondo la c.d. "cultura del mero adempimento", ma richiedono alle stesse un ruolo proattivo e concreto ispirato al principio di *accountability* (che possiamo tradurre come "responsabilizzazione" o "responsabilità"). Muta, quindi, la filosofia di fondo nel trattamento dei dati personali, si passa cioè a un approccio fondato sull'*accountability*, tutto ciò comporta la modifica nella *governance*: le questioni relative al trattamento dei dati diventano questioni soprattutto di gestione del rischio. L'applicazione del RGPD interviene su più livelli: normativo, organizzativo, contrattuale, tecnologico, comunicativo. Interventi finalizzati a bilanciare la libera circolazione dei dati e i diritti fondamentali delle persone fisiche.

2. *Accountability (Responsabilizzazione / Responsabilità del Titolare) e principi applicabili di trattamento dei dati personali*

Il principio di *accountability* non rappresenta una novità assoluta nell'ambito del trattamento dei dati personali, essendo già stato oggetto di un interessante parere (n. 3/2010 sul principio di responsabilità, adottato il 13 luglio 2010) del Gruppo di lavoro Articolo 29 per la protezione dei dati. Nel succitato parere il Gruppo di lavoro ex art. 29 si soffermava sulla necessità che la protezione dei dati dovesse passare, quanto prima, "dalla teoria alla pratica". Pertanto, gli obblighi giuridici dovevano essere tradotti in misure concrete di protezione dei dati, per favorire la protezione dei dati nella pratica, il quadro giuridico dell'Unione europea doveva introdurre dei meccanismi aggiuntivi. Al riguardo, furono subito proposti nuovi istituti basati sulla responsabilità, come mezzo per incoraggiare i responsabili del trattamento ad attuare strumenti pratici e operativi per garantire una più efficace protezione dei dati: "Un principio di responsabilità vincolante imporrebbe esplicitamente ai responsabili del trattamento di attuare misure appropriate ed efficaci per dare applicazione ai principi e agli obblighi della direttiva, e per dimostrarne su richiesta l'osservanza. In pratica, ciò dovrebbe concretarsi in programmi improntati all'adattabilità mirati ad attuare i principi esistenti di protezione dei dati (talvolta denominati "programmi di conformità").

Quale complemento a tale principio, potrebbero essere istituiti obblighi aggiuntivi diretti ad attuare garanzie di protezione dei dati o ad assicurarne l'efficacia. Potrebbe trattarsi, per esempio, di una disposizione che obbliga a effettuare una valutazione d'impatto sulla privacy per le operazioni di trattamento di dati a più alto rischio"[4].

Con il progressivo effetto diluvio di dati, dovuto al continuo e inarrestabile aumento di quantità dei dati personali oggetto di trattamento mediante i più disparati dispositivi, sono aumentati drasticamente anche i rischi di abuso e di trattamento illecito degli stessi. Da qui la necessità che anche nel settore pubblico vengano attuati meccanismi reali ed efficaci per tutelare le informazioni personali. L'architettura giuridica dei meccanismi di responsabilità, delineata dal Gruppo ex Art. 29, sarebbe basata su due livelli: il primo livello sarebbe rappresentato da un obbligo vincolante per tutti i titolari del trattamento. Detto obbligo comprenderebbe due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove. "Il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure (norme di attuazione eccedenti il livello minimo)"[5].

Sotto il profilo terminologico, il termine inglese "accountability" (responsabilità) proviene dal mondo anglosassone, dove è di uso comune e dove il suo significato è ampiamente compreso e condiviso. "Ciononostante, risulta complesso definire che cosa esattamente significhi "accountability" in pratica. In generale, comunque, l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente. Nella maggior parte delle altre lingue europee, principalmente a causa delle differenze tra i sistemi giuridici, il termine "accountability" non è facilmente traducibile. Di conseguenza, il rischio di un'interpretazione variabile del termine, e quindi di una mancanza di armonizzazione, è sostanziale"[6].

Per addivenire a una proposta concreta, il Gruppo ex Art. 29 prevede che il principio generale di responsabilità avrebbe lo scopo di promuovere l'adozione di misure concrete e pratiche, in quanto trasformerebbe i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del titolare del trattamento, nel rispetto delle leggi e dei regolamenti applicabili. Il titolare del trattamento dovrebbe anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. Una disposizione generale di questo tipo si incentrerebbe su due elementi principali: 1) la necessità che il titolare del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati; 2) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile del trattamento deve fornire la prova di quanto esposto al punto 1.

Il principio generale di responsabilità sopra richiamato evita volutamente di precisare la tipologia di misura da attuare. Tutto ciò solleva due questioni di fondamentale importanza: 1) quali misure comuni soddisferebbero il principio di responsabilità? 2) Con quali modalità graduare e adattare le misure a circostanze specifiche? Al riguardo il Gruppo ex Art. 29 presenta un lungo elenco di misure comuni, che i titolari del trattamento dovrebbero adottare per ottemperare alla prima parte del principio di responsabilità. L'idoneità delle misure andrà valutata caso per caso per caso. Le misure specifiche da attuare dovranno essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare riferimento al rischio relativo al trattamento e alla tipologia di dati. Seguendo tale approccio, i titolari del trattamento devono essere in grado di adattare le misure alle specificità concrete delle loro situazioni particolari e delle operazioni di trattamento dei dati in questione.

Ciò vuol dire che non si deve partire

[4] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010 sul principio di responsabilità*, adottato il 13 luglio 2010, 3.

[5] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010*, 6.

[6] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010*, 6.

semplicemente dal precetto normativo, ma dalla finalità cui tende la disposizione normativa, ossia la tutela del dato personale per poi individuare in concreto le misure da adottare in conformità con il RGPD. Si parte, quindi, dalla costruzione di un sistema di misure da parte del titolare del trattamento che deve essere in grado di garantire il rispetto dei diritti fondamentali dell'individuo alla protezione dei dati personali. Al riguardo, il RGPD non indica le misure da adottare, ma solo i principi da seguire per conseguire l'obiettivo fondamentale, ossia: la tutela dei dati personali.

Il RGPD è diventato pienamente operativo il 25 maggio 2018, ma le norme di adeguamento sono state emanate con il d.lgs. 10 agosto 2018, n. 101, con il decreto legge 8 ottobre 2021, n. 139 (convertito con modificazioni dalla legge 3 dicembre 2021, n. 205 e dal decreto legge 30 settembre 2021 n. 132 (convertito con modificazioni dalla legge 23 novembre 2021, n. 178) con i quali viene abrogato o modificato parte del precedente quadro normativo, il D.lgs, n.196/2003. Dal 2018 tutta la disciplina italiana dovrà essere interpretata alla luce del RGPD. Il regolamento europeo in materia di protezione dei dati personali diventa quindi la fonte del diritto per tutte le norme nazionali.

"Dal punto di vista della tecnica normativa si è novellato il Codice privacy previgente, pur nella consapevolezza che il Regolamento ha sostanzialmente modificato la prospettiva dell'approccio alla tutela della privacy, essendo informato ad una filosofia diversa rispetto a quella del vecchio Codice. Il nuovo approccio al rischio dettato dal legislatore europeo è, infatti, basato su numerosi istituti che si iscrivono in una prospettiva di carattere responsabilizzante, volta a trasformare la *compliance* privacy da adempimento normativo a sistema di gestione, che potremmo sintetizzare nel principio dell'a*ccountability* –ossia nella capacità di rendere conto– volto a valorizzare in capo ai *data controller* l'adozione di comportamenti proattivi, consistenti nell'obbligo per il titolare del trattamento non tanto di conformarsi passivamente a regole dettate dall'esterno, la cui osservanza formale potrebbe non rappresentare una garanzia effettiva, bensì di adottare le misure più efficaci per attuare i principi che presidiano alla protezione dei dati personali ed, all'occorrenza, dare conto ("rendicontare") delle misure giuridiche, organizzative e tecniche concretamente adottate. Pertanto, il Regolamento non effettua la scelta in molti casi specifici, ma la rimette al titolare del trattamento che è chiamato ad effettuare una valutazione, ad assumere una decisione e a provare di aver adottato misure proporzionate ed efficaci"[7].

Il Parlamento aveva raccomandato un'entrata in vigore soft della nuova disciplina, ma il d.lgs. n. 101/2018 non ha accolto tale raccomandazione. In sostanza con il d.lgs. 101/2018 si completa il percorso di armonizzazione che porta a un sistema normativo a due livelli in materia di trattamento dei dati personali. Il primo livello è quello europeo, ed è costituito dal RGPD. Quest'ultimo è la norma di fonte superiore, cui la disciplina nazionale deve allinearsi in base al principio della gerarchia delle fonti del diritto. Il secondo livello è rappresentato dal Codice per la protezione dei dati personali, emanato con il d.lgs. n. 196/2003 e modificato con il d.lgs. 101/2018. Il codice in materia di protezione dei dati personali raccoglie la normativa vigente in materia accumulatosi dal 1996 e la adegua alle disposizioni del RGDP.

Com'è noto, il RGPD è direttamente applicabile dal 25 maggio 2018. L'adeguamento dell'ordinamento italiano doveva essere coerente temporalmente con tale data. Al riguardo, la legge di delegazione europea ha stabilito, all'art. 13, comma 3, i seguenti criteri che devono ispirare il nostro legislatore:

"a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) modificare il codice di cui al d.lgs. 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati

[7] F. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, n. 22, 2018, 31.

personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse".

Oltre a ciò, fra i principi e criteri direttivi generali di cui all'art. 32 della legge 24 dicembre 2012, n. 23, sono indicati quelli del riassetto e della semplificazione normativi con l'indicazione esplicita delle norme abrogate.

Gran parte delle disposizioni del Codice è stata abrogata espressamente per essere risultate incompatibili con quelle contenute nel RGPD; norme che, a loro volta, sono per la maggior parte direttamente applicabili e costituiranno per il futuro il regime primario interno circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché circa la libera circolazione degli stessi dati. Altra e minore parte delle previsioni codicistiche nazionali è stata modificata in modo rilevante, in relazione a disposizioni del RGPD non direttamente applicabili, e che segnatamente lasciavano spazi all'intervento degli Stati membri, in particolare tramite il legislatore nazionale. In questo secondo caso, si è deciso di intervenire direttamente sul Codice introducendo nuove disposizioni o modificando quelle già presenti.

Codice e RGPD sono informati a due filosofie diverse. Il RGPD, come già rilevato, è basato sulla cosiddetta *accountability*, (responsabilità/responsabilizzazione). Questa consiste nell'obbligo per il titolare del trattamento di adottare misure appropriate ed efficaci per attuare i principi di protezione dei dati, nonché nella necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci.

Dunque il regolamento non effettua la scelta in molti casi specifici, ma la rimette al titolare del trattamento che è chiamato ad effettuare una valutazione, ad assumere una decisione e a provare di avere adottato misure proporzionate ed efficaci.

Il RGPD, facendo propria questa visione, pone, come anticipato, l'accento sulla responsabilizzazione dei titolari e dei responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione delle disposizioni regolamentari. Viene, quindi, affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati, ovviamente nel rispetto della normativa e dei criteri previsti dal RGPD.

Il primo fra questi criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto previsto dall'art. 25 del RGPD) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel RGPD rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (in particolare, considerando 75-77[8]); tali impatti dovranno essere analizzati

[8] Considerando (75) "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di

attraverso un apposito processo di valutazione (si vedano artt. 35-36), c.d. valutazione d'impatto, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (al riguardo, di particolare importanza sono le linee-guida in materia di valutazione di impatto sulla protezione dei dati adottate dal Gruppo "Articolo 29). All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare i rischi) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58, cioè dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Il principio di responsabilizzazione impone al titolare l'adozione del registro dei trattamenti (ai sensi dell'art. 30), di approntare misure di sicurezza che debbano "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza, poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del RGPD. La nuova normativa prevede la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

In ogni caso, il Garante per la protezione dei dati personali potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti nel corso di questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del RGPD) potranno restare in vigore (in base all'art. 6, paragrafo 2, del RGPD) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi, ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto qualora ritengano probabile che da tale violazione possano derivare rischi per i diritti e le libertà degli interessati (considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice in materia di protezione dei dati personali. I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del RGPD. Al riguardo, di particolare rilievo sono le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo

persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati". Considerando (76) "La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato". Considerando (77) Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio".

"Articolo 29" (*Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679, adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 versione emendata e adottata il 6 febbraio 2018*). Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (art. 33, paragrafo 5).

Anche la designazione di un "Responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: *Data Protection Officer*) riflette l'approccio responsabilizzante che è proprio del RGPD (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35.

Il RGPD (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è appunto il principio detto di "responsabilizzazione" (o *accountability*), il quale richiede la messa in atto da parte del titolare di tutte le misure sopra citate; principio che viene poi esplicitato ulteriormente dall'art. 24, paragrafo 1, del RGPD, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento".

Alla luce anche del principio di *accountability*, ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, ossia: liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato; limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati; minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento; esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento; limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento; integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Una delle misure più importanti e concrete, nell'ambito del principio di responsabilizzazione, che il titolare del trattamento deve porre in essere riguarda la trasparenza delle attività di trattamento dati che pone in essere.

3. *Trasparenza nel trattamento dei dati personali da parte delle Amministrazioni Pubbliche*

Chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni, anche per metterlo nelle condizioni di esercitare i propri diritti, previsti agli artt. 15-22 del RGPD. Il principio di trasparenza[9], inteso come obbligo di rendere conoscibili le modalità con cui i dati sono raccolti, utilizzati e consultati grazie a comunicazioni e informazioni facilmente accessibili e comprensibili, utilizzando un linguaggio chiaro e semplice (considerando 39)[10], ha nel RGPD un ruolo fondamentale e

[9] M. Dell'Utri, *Il principio di trasparenza*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, 199; F. Pizzetti, *Trasparenza nel trattamento dati, che cambia col GDPR: l'alba di un nuovo valore sociale*, in *Agenda Digitale*, 2018 (*https://www.agendadigitale.eu/sicurezza/trasparenza-nel-trattamento-dati-che-cambia-col-gdpr-lalba-di-un-nuovo-valore-sociale/*).

[10] Considerando (39) "Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero es-

potenzialmente molto espansivo.

La trasparenza è un obbligo trasversale a norma del RGPD, che si esplica in tre elementi centrali: 1) la fornitura agli interessati d'informazioni relative al trattamento corretto; 2) le modalità con le quali il titolare del trattamento comunica con gli interessati riguardo ai diritti di cui godono ai sensi del regolamento; 3) le modalità con le quali il titolare del trattamento agevola agli interessati l'esercizio dei diritti di cui godono. Il Gruppo di lavoro Articolo 29 ha adottato, al riguardo, le Linee guida sulla trasparenza ai sensi del Regolamento 2016/679, adottate il 29 novembre 2017 ed emendate l'11 aprile 2018.

Dette linee guidano mirano, soprattutto, a consentire ai titolari del trattamento di comprendere, a un livello elevato, come il Gruppo interpreti gli effetti pratici degli obblighi di trasparenza e a indicare l'approccio che, secondo il Gruppo, i titolari del trattamento devono adottare per essere trasparenti, ricomprendendo al contempo correttezza e responsabilizzazione nelle loro misure di trasparenza.

La trasparenza è un aspetto che da tempo si è radicato nel diritto dell'Unione europea. È finalizzata infondere fiducia nei processi che riguardano i cittadini, permettendo loro di comprenderli e, se necessario, di opporvisi. Inoltre, è espressione del principio di correttezza in relazione al trattamento dei dati personali affermato all'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Ai sensi dell'art. 5, paragrafo 1, lettera a), del RGPD, oltre ai requisiti che il trattamento dei dati sia lecito e corretto, la trasparenza è ora inclusa in quanto elemento fondamentale di questi principi, questa, infatti, è intrinsecamente legata alla correttezza e al nuovo principio di responsabilizzazione ai sensi del RGPD. Il titolare del trattamento dev'essere sempre in grado di dimostrare che i dati personali sono trattati in modo trasparente nei confronti dell'interessato (art. 5, paragrafo 2, RGPD). A questo si aggiunge il fatto che il principio di responsabilizzazione impone la trasparenza delle operazioni di trattamento affinché il titolare del trattamento sia in grado di dimostrare il rispetto degli obblighi che il regolamento gli impone.

Secondo il considerando 171 del RGPD, laddove il trattamento fosse stato già in corso prima del 25 maggio 2018, il titolare del trattamento avrebbe dovuto garantirne la conformità agli obblighi di trasparenza alla data del 25 maggio 2018 (così come a tutti gli altri obblighi previsti dal regolamento). Ciò significa che prima del 25 maggio 2018 il titolare del trattamento avrebbe dovuto revisionare tutte le informazioni fornite agli interessati con riferimento al trattamento dei dati personali che li riguardano (ad esempio in dichiarazioni/informative sulla privacy, ecc.), al fine di garantire l'adempimento degli obblighi di trasparenza esaminati nelle citate linee guida.

Quando il titolare del trattamento la rispetta, la trasparenza consente agli interessati di imputare la responsabilità al titolare e al responsabile del trattamento e di esercitare il controllo sui dati personali che li riguardano, ad esempio dando o revocando il consenso informato e attivando i loro diritti di interessati.

Gli obblighi d'informazione sono specificamente indicati negli artt. 12-14 del RGPD. La qualità, l'accessibilità e la comprensibilità delle informazioni sono i requisiti fondamentali in grado di garantire la trasparenza del trattamento e fornire indicazioni concrete circa il principio di finalità alla base di ogni trattamento dati.

Gli obblighi di trasparenza imposti dal regolamento si applicano a prescindere dalla base giuridica del trattamento e per tutto il ciclo di vita dello stesso. Ciò risulta chiaro dall'art. 12, il quale stabilisce che la trasparenza si applica nelle seguenti fasi del ciclo di trattamento dei dati:

- prima o all'inizio del ciclo di trattamento dei dati, vale a dire quando i dati personali sono raccolti presso l'interessato od ottenuti in altro modo;
- nell'arco dell'intero ciclo di vita del trattamento, ovvero nella comunicazione con gli interessati sui loro diritti;

sere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento".

- in momenti specifici in cui il trattamento è in corso, ad esempio quando si verifica una violazione di dati oppure in caso di modifica rilevante del trattamento.

Il concetto di trasparenza non viene definito all'interno del regolamento. Il considerando 39 del RGPD, come già rilevato, ne illustra il significato e l'effetto nell'ambito del trattamento dei dati.

L'art. 12 del RGPD fissa le regole generali che si applicano alla fornitura delle informazioni agli interessati (ai sensi degli artt. 13 e 14 del RGPD), alla comunicazione con gli interessati riguardo all'esercizio dei loro diritti (ai sensi degli artt. 15-22 del RGPD) e alle comunicazioni relative alle violazioni di dati (art. 34 del RGPD). In particolare, l'articolo 12 impone che le informazioni o le comunicazioni in questione debbano rispettare i criteri seguenti: devono essere concise, trasparenti, intelligibili e facilmente accessibili; devono essere formulate con un linguaggio semplice e chiaro; il requisito di un linguaggio semplice e chiaro è di particolare importanza nel caso d'informazioni destinate ai minor; devono essere fornite per iscritto "o con altri mezzi, anche, se del caso, con mezzi elettronici"; se richiesto dall'interessato, possono essere fornite oralmente; devono essere in genere gratuite.

L'obbligo di fornire agli interessati le informazioni e le comunicazioni in forma "concisa e trasparente" implica che il titolare del trattamento presenti le informazioni/comunicazioni in maniera efficace e succinta al fine di evitare il c.d. "subissamento" informativo. Tali informazioni dovrebbero essere differenziate nettamente da altre che non riguardano la vita privata, quali clausole contrattuali o condizioni generali d'uso. Nell'ambiente online l'utilizzo di una dichiarazione/informativa sulla privacy stratificata può consentire all'interessato di consultarne immediatamente la specifica sezione desiderata, senza dover scorrere ampie porzioni di testo alla ricerca di un argomento in particolare.

L'obbligo di fornire informazioni "intelligibili" implica che queste debbano risultare comprensibili a un esponente medio del pubblico cui sono dirette. L'intelligibilità è strettamente connessa all'obbligo di utilizzare un linguaggio semplice e chiaro. Il titolare dei dati responsabilizzato saprà su che tipo di persone raccoglie informazioni e potrà utilizzare tali conoscenze per stabilire che cosa è probabile che il pubblico in questione comprenda.

Un aspetto fondamentale del principio della trasparenza messa in luce nelle linee guida risiede nel fatto che l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano Ciò costituisce un aspetto importante del principio di correttezza di cui all'articolo 5, paragrafo 1, del regolamento ed è altresì connesso al considerando 39, il quale stabilisce che "[è] opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali...".

L'elemento della "facile accessibilità" implica che l'interessato non sia costretto a cercare le informazioni, ma che anzi gli sia immediatamente chiaro dove e come queste siano accessibili.

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del RGPD) deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati (se raccolti direttamente presso l'interessato, art. 13 del RGPD).

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del RGPD), l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).

I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13, paragrafo 1, e 14, paragrafo 1, del RGPD e, in parte, sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD (Responsabile della protezione dei dati), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Se i dati non sono raccolti direttamente presso

l'interessato (art. 14 del RGPD), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

Il Regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Qualora il trattamento contemplasse processi decisionali automatizzati (anche la profilazione), l'informativa dovrebbe specificarlo e dovrebbe indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: art. 12, paragrafo 1, e considerando 58 del RGPD). Sono comunque ammessi "altri mezzi", quindi può essere fornita anche in forma orale, ma nel rispetto delle caratteristiche di cui sopra rappresentate (art. 12, paragrafo 1, RGPD).

Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone in futuro dovranno essere uniformate in tutta l'Ue attraverso l'intervento dalla Commissione europea.

In base al Regolamento, si deve porre particolare attenzione alla formulazione dell'informativa, che deve essere soprattutto comprensibile e trasparente per l'interessato, attraverso l'uso di un linguaggio chiaro e semplice. Per quanto riguarda i minori devono essere predisposte idonee informative (Considerando 58)[11].

La prospettiva da cui parte la nuova disciplina europea in materia di protezione dei dati personali è quella del "nuovo mondo digitale", le cui insidie sono rinvenibili non solo nel trattamento dei dati ma anche negli effetti da esso derivanti. In tal senso, si è spesso fatto ricorso proprio ai principi di trasparenza e lealtà del trattamento per chiedere che le informative fornite agli utenti consentissero di comprendere in modo adeguato non solo le modalità di trattamento, potevano verificarsi rispetto agli interessati e agli utenti[12].

4. *Il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri come base giuridica*

Dalla lettura del RGPD emerge chiaramente come, nel caso del titolare del trattamento sia un soggetto pubblico, presupposti e modalità del trattamento si differenzino da quelli che presiedono al trattamento operato da soggetti privati. Il primo elemento saliente concerne proprio la possibile base giuridica del trattamento. Nel caso delle amministrazioni pubbliche, infatti, questa può essere data non solo dal consenso o dall'esistenza di un obbligo legale, ma anche dalla necessità del trattamento per "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Al riguardo l'art 2-ter del Codice prevede che: la base giuridica prevista dall'art. 6, par. 3, lettera b), del regolamento è costituita da una norma di legge o di regolamento o da atti amministrativi generali. Fermo restando ogni altro obbligo previsto dal Regolamento e dal Codice, "il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi

[11] Considerando (58) "Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente".

[12] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016; C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018.

comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nonché da parte di una società a controllo pubblico statale o, limitatamente ai gestori di servizi pubblici, locale, di cui all' articolo 16 del testo unico in materia di società a partecipazione pubblica, di cui al decreto legislativo 19 agosto 2016, n. 175 , con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato, è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento"[13].

Se il trattamento per l'esecuzione di un interesse pubblico o per l'esercizio di pubblici poteri è un requisito alternativo all'obbligo legale, ciò significa che la valutazione della necessarietà può essere rimessa all'amministrazione procedente, alla quale la legge ha assegnato il potere di curare l'interesse pubblico in una data materia o per una determinata funzione.

L'interpretazione letterale non offre ragioni per ritenere superato quanto ritenuto prima delle modifiche introdotte al Codice, in merito alla possibilità di trattare dati personali "comuni" da parte di soggetti pubblici anche in assenza di una legge che lo preveda espressamente[14]. Al contrario, si può legittimamente ravvisare nello stesso art. 5 del RGPD la base giuridica "sufficiente per rientrare nel rispetto del principio di legalità dell'azione amministrativa e del fondamento legittimo previsto dalla legge richiesto per il trattamento dei dati personali dall'art. 8 della Carta dei diritti fondamentali UE, nel senso di consentire alla pubblica amministrazione di trattare dati semplici o ordinari, per i quali non c'è un esplicito divieto di trattamento, per finalità di interesse pubblico; e di ricondurre in tal caso nell'ambito e nei limiti del principio di proporzionalità dell'attività amministrativa le previsioni recate dall'art. 6 per il trattamento di dati ordinari o semplici"[15].

La comunicazione[16] fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del RGPD e di quelli relativi a condanne penali e reati di cui all'art. 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa "se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis" del Codice.

Al riguardo, il Garante per la protezione dei dati personali ha precisato che "Ai sensi della disciplina in materia, il trattamento di dati personali effettuato in ambito pubblico è lecito solo se tale trattamento è necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" oppure "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6, par. 1, lett. c) ed e)). Al riguardo, si evidenzia che la comunicazione di dati personali – ossia "il dare conoscenza dei dati personali a uno o più soggetti determinati

[13] Sul punto, F. Cardarelli, *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. Finocchiaro, R. D'Orazio, O. Pollicino e G. Resta (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè 2021: "L'art. 6 del Regolamento elenca sei basi giuridiche (le quali rappresentano quindi i presupposti di legittimazione del trattamento) che rendono lecito e legittimo, fin dall'origine, il trattamento di dati "comuni". Tale disposizione, riprendendo quasi integralmente le previsioni dell'art. 7 della dir. 95/46/CE, àncora la liceità del trattamento alla sussistenza di presupposti che si fondano due requisiti generali alternativi (il consenso dell'interessato — par. 1, lett. a — oppure la necessità del trattamento — par. 1, lett. b-f). Tra queste ipotesi di trattamento necessario le lett. c) ed e) della disposizione contemplano "c) l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento", "e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

[14] F. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 4 ss.

[15] F. Francario, *Protezione dei dati personali e pubblica amministrazione*, in C. Pisani, G. Proia e A. Topo (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022.

[16] Per comunicazione si intende: "Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione" (Art. 2 – ter, comma 4 lett. a), D.lgs. n. 196/2003).

diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'art. 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione" – diversi da quelli previsti dagli artt. 9 e 10 del Regolamento (UE) 2016/679, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, è ammessa se prevista esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-ter del Codice). Con riguardo alle categorie particolari di dati personali, inclusi quelli relativi alla salute (in merito ai quali è previsto un generale divieto di trattamento, ad eccezione dei casi indicati all'art. 9, par. 2 del Regolamento e, comunque, un regime di maggiore garanzia rispetto alle altre tipologie di dati, in particolare, per effetto dell'art. 9, par. 4, nonché dell'art. 2-septies del Codice), il trattamento è consentito, quando "necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. g), del Regolamento). Il legislatore nazionale ha definito "rilevante" l'interesse pubblico per il trattamento "effettuato da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri" nelle materie indicate, seppur in modo non esaustivo, dall'art. 2-sexies del Codice, stabilendo che i relativi trattamenti "sono ammessi qualora siano previsti […] da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato". Il trattamento dei dati personali deve inoltre avvenire nel rispetto dei principi indicati nell'art. 5 del Regolamento, fra cui quelli di "liceità, correttezza e trasparenza" nonché di "minimizzazione dei dati", secondo i quali i dati personali devono essere – rispettivamente – "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" nonché "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5 par. 1, lett. a) e c)"[17].

La diffusione[18] e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente "se previste ai sensi del comma 1 o se necessarie ai sensi del comma 1-bis" del Codice. In tale ultimo caso, ne viene data notizia al Garante per la protezione dei dati personali almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

4.1. *Il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*

Come chiarito nei capitoli che precedono, quei dati che un tempo denominavamo dati sensibili, con l'entrata in vigore del RGPD hanno cambiato nome. Adesso sono denominati "dati particolari" e sono una tipologia della più ampia categoria dei dati personali. Secondo l'art. 9, par. 1, del RGPD, è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il trattamento di dati particolari da parte della PA, così come previsto dall'art. 9, par. 2, lett. g) GDPR, è ammesso solo se è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Il Legislatore nazionale, mediante il D.lgs. 101/2018, ha previsto all'art. 2-sexies, rubricato

[17] Garante per la protezione dei dati personali, 25 febbraio 2021, (doc. web n. 9565218).

[18] Per diffusione si intende: "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione" (Art. 2 – ter, comma 4 lett. b), D.lgs. n. 196/2003).

"Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante" che: "I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. 2. Fermo restando quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: accesso a documenti amministrativi e accesso civico; tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità; tenuta di registri pubblici relativi a beni immobili o mobili; tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli; cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato; elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari; Garante per la protezione dei dati personali esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche; svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo; attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale; attività di controllo e ispettive; concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni; conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali; rapporti tra i soggetti pubblici e gli enti del terzo settore; obiezione di coscienza; attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose; attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci; attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano; compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale; vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili; bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario; cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione,

l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati Garante per la protezione dei dati personali dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan); dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva". Occorre evidenziare che tale elenco deve intendersi come esemplificativo e non esaustivo e il riferimento alla base giuridica dell'interesse pubblico rilevante ha un forte ancoraggio al principio di legalità sostanziale. Pertanto, l'art. 2-sexies del Codice si sofferma diffusamente sul trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante.

5. *Il Responsabile della Protezione dei Dati nelle Amministrazioni Pubbliche*

Il RGPD fondato, come già più volte messo in luce, sul principio di accountability, delinea, in parte, un nuovo quadro giuridico e pone al centro di questo la figura del Responsabile della protezione dei dati (d'ora in poi, RPD). Questa figura non rappresenta una novità assoluta nel panorama europeo, dato che in molti Stati membri, pur non essendo prevista dalla direttiva 95/46/CE, la nomina del RPD è divenuta, nel corso degli anni, una prassi. Anche la Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, contempla all'art. 32 la designazione del RPD: "Gli Stati membri dispongono che il titolare del trattamento designi un responsabile della protezione dei dati. Gli Stati membri possono esentare le autorità giurisdizionali e le altre autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali da tale obbligo".

Il Gruppo Articolo 29 per la protezione dei dati personali ha più volte sottolineato, prima dell'adozione del RGPD, che la figura del RPD rappresenta un elemento chiave all'interno del nuovo sistema di governance dei dati e una figura fondamentale ai fini della "responsabilizzazione", e che tale nomina possa rendere più agevole l'applicazione della normativa: "oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente"[19].

Il RGPD (considerando 97) prevede che "per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali

[19] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Linee guida sui responsabili della protezione dei dati, adottate il 13 dicembre 2016*, versione emendata e adottata in data 5 aprile 2017.

responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

Ai sensi dell'art. 37, par.1, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici: a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico; b) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; c) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, sono quindi obbligati a nominare un RPD. Al riguardo, l'art. 37, par. 1, lett. a), del RGPD prevede che i titolari e i responsabili del trattamento designino un RPD "quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali". L'atto di designazione è parte costitutiva dell'adempimento. Il RGPD non fornisce la definizione di "autorità pubblica" o "organismo pubblico" e, come chiarito anche nelle Linee guida adottate in materia dal Gruppo Art. 29 (Linee guida sui responsabili della protezione dei dati, adottate il 5 aprile 2017), ne rimette l'individuazione al diritto nazionale applicabile. Allo stato, in ambito pubblico, secondo le indicazioni fornite dal Garante per la protezione dei dati personali[20], devono ritenersi tenuti alla designazione di un RPD i soggetti che oggi ricadono nell'ambito di applicazione degli artt. 18 – 22[21] del Codice in materia di protezione dei dati personali, che stabiliscono le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio: le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.). Al riguardo, occorre richiamare la nozione di "organismo pubblico" come definita al par. 1.3 dell'Allegato alla Raccomandazione n. R (91) 10 del Comitato dei Ministri del Consiglio d'Europa, adottata il 9 settembre 1991: "l'espressione organismi pubblici indica qualsiasi amministrazione, istituzione, ente o altra entità che eserciti funzioni di servizio pubblico o di interesse pubblico tramite prerogative proprie dei pubblici poteri". Una definizione di "ente pubblico" e di "organismo di diritto pubblico" possiamo rinvenirla anche nell'art. 1, par. 1 e 2, della direttiva 2003/98/CE.

Il Garante raccomanda però che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), sarebbe auspicabile, ancorché non obbligatorio, che anche detti soggetti procedessero alla designazione di un RPD.

Qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti (in termini di criteri per la designazione, posizione e compiti) che valgono per i RPD designati in via obbligatoria.

Come già rilevato, nel RGPD non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo Art. 29, nelle predette Linee guida, precisa che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico. In questi casi la nomina di un RPD è obbligatoria. E, al riguardo, aggiunge che "lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di

[20] Garante per la protezione dei dati personali, Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29), www.garanteprivacy.it, docweb 7322110.

[21] Sul punto, P. Troiano, *Art. 18 – Regole applicabili a tutti i trattamenti effettuati da soggetti pubblici*, in C.M. Bianca e F.D. Busnelli (a cura di), *La protezione dei dati personali*, Padova, Cedam, 2007, 456-474.

disciplina professionale. In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD". Anche se nei casi sopra riportati non sussista l'obbligo di nominare un RPD, il Gruppo di lavoro consiglia che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD.

Con l'espressione "attività principali", sempre secondo il Gruppo Art. 29, possiamo intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento. Detta espressione ("attività principali") non va, ovviamente, interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisca una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento.

L'art. 37 del RGPD fa riferimento, per la nomina obbligatoria del RPD, al trattamento di dati personali su "larga scala". Nel regolamento non figura alcuna definizione di trattamento su "larga scala". Il considerando 91 fornisce, però, alcune indicazioni al riguardo: per trattamenti su "larga scala" si intendono quelli "che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". Pertanto, al fine di stabilire se un trattamento sia effettuato su larga scala è necessario tener conto: del numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; del volume dei dati e/o delle diverse tipologie di dati oggetto di trattamento; della durata, ovvero la persistenza, dell'attività di trattamento; della portata geografica dell'attività di trattamento.

Il RGPD non si sofferma neppure sul concetto di "monitoraggio regolare e sistematico", al riguardo giova riprendere quanto affermato, nelle predette Linee guida, dal Gruppo Art. 29: "Il considerando 24 menziona il monitoraggio del comportamento di detti interessati ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati. L'aggettivo regolare ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; ricorrente o ripetuto a intervalli costanti; che avviene in modo costante o a intervalli periodici. L'aggettivo sistematico ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolto nell'ambito di una strategia". Alcuni esempi di attività che possono comportare il "monitoraggio regolare e sistematico" di interessati possono essere: "curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.".

Per quanto riguarda la nomina di un RPD, l'art. 37 non distingue fra titolari del trattamento e responsabili del trattamento in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione. Tra

l'altro, qualora il titolare del trattamento sia tenuto, in base ai succitati criteri, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina, che però può costituire una buona prassi.

L'art. 37, par. 2, del RGPD, permette la designazione di un unico RPD per più organismi (es. gruppo imprenditoriale) a condizione che il responsabile sia "facilmente raggiungibile da ciascuno stabilimento". Ovviamente, il concetto di "raggiungibilità" è riferito ai compiti del RPD in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente, dato che uno dei compiti del RPD, ai sensi dell'art. 39, p. 1, lett. a), consiste "nell'informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento". Il RPD deve essere in grado di comunicare con gli interessati in modo efficiente. Al riguardo, appare opportuno ricordare quanto previsto dall'art. 12, par. 1, del RGPD "Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori". Il RPD deve essere anche in grado di comunicare e collaborare con le autorità di controllo interessate. L'art. 37, par. 3, consente la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenendo sempre presente la loro struttura organizzativa e la dimensione. Il titolare o il responsabile, poiché il RPD è chiamato a una molteplicità di funzioni, deve assicurarsi che un unico RPD, se necessario supportato da un gruppo di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

Il RPD è designato in funzione delle qualità professionali, "in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39" (art. 37, par. 5, RGPD). Al riguardo, il considerando 97 prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

Il livello di conoscenza specialistica richiesto, come fatto giustamente rilevare nelle Linee guida del Gruppo Art. 29, non trova una definizione tassativa. Pertanto, andrebbe proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. "Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi".

Il RGPD all'art. 37, par. 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un RPD. Al riguardo, sarebbe necessario prendere in considerazione la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD. Viene considerata utile anche la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento, nonché una conoscenza delle operazioni di trattamento svolte con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare. Negli ultimi tempi spesso ci si è chiesti quali certificazioni risultino idonee a legittimare il RPD nell'esercizio delle sue funzioni, ai sensi degli artt. 42 e 43 del RGPD. Il Garante per la protezione dei dati personali ha ritenuto opportuno precisare che "come accade nei settori delle cosiddette professioni non regolamentate, si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del RGPD) sono rilasciate anche all'esito della partecipazione ad attività formative e al controllo dell'apprendimento. Esse, pur rappresentando, al pari di altri titoli,

un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD".

Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

Il RPD deve essere in grado di assolvere i propri compiti, tenendo conto delle qualità personali e delle sue conoscenze, nonché della posizione dello stesso all'interno dell'amministrazione. Il RPD svolge un ruolo chiave, di assoluta centralità, nel promuovere la cultura della protezione dei dati all'interno dell'amministrazione, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

Il titolare del trattamento e il responsabile del trattamento devono assicurare che il RPD sia "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali". Il RPD va coinvolto, infatti, in ogni questione relativa alla protezione dei dati personali: "Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il RPD vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni. Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento. Ciò significa che occorrerà garantire, per esempio: che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello; la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea; che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il Gruppo di lavoro raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD; che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente".

L'art. 38, par. 2, del RGPD prevede che il titolare del trattamento o il responsabile del trattamento debbano adeguatamente sostenere il RPD "fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".

Il RPD deve poter operare con una certa autonomia all'interno dell'organizzazione del titolare o del responsabile, questi non deve, infatti, ricevere alcuna istruzione per quanto riguarda l'esecuzione dei compiti ad egli demandati. I RPD "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente" (Considerando 97). Nell'esecuzione dei compiti attribuitigli dall'art. 39, il RPD non deve ricevere istruzioni sull'approccio da seguire nel caso specifico, quali siano i risultati attesi, come eventualmente condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo, né ricevere istruzioni sull'interpretazione da fornire a una specifica questione in tema di protezione dati. I margini decisionali del RPD sono ben delineati nell'art. 39 del RGPD. Sul punto rilevano correttamente le Linee guida del Gruppo Art. 29 che "Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza. Se il titolare del trattamento o il responsabile del trattamento assumono decisioni incompatibili con il RGPD e le

indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'articolo 38, paragrafo 3, prevede che il RPD riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel quadro delle sue funzioni di informazione e consulenza a favore del titolare del trattamento o del responsabile del trattamento. Un altro esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico".

L'art. 38, par. 3, del RGPD mira a potenziare ulteriormente l'autonomia e l'indipendenza del RPD prevedendo che non debba essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. In base all'art. 38, par. 6, al RPD è consentito di "svolgere altri compiti e funzioni", ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che "tali compiti e funzioni non diano adito a un conflitto di interessi".

A seconda della natura dei trattamenti e delle attività e dimensioni della struttura del titolare o del responsabile, le eventuali ulteriori incombenze attribuite al RPD non dovrebbero pertanto sottrarre allo stesso il tempo necessario per adempiere alle relative responsabilità.

"In linea di principio, è quindi ragionevole che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al RPD ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle asl). In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, l'attribuzione delle funzioni di RPD al responsabile per la prevenzione della corruzione e per la trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti che il RGPD attribuisce al RPD" (Garante per la protezione dei dati personali, Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico, www.garanteprivacy.it, docweb 7322110).

Tra i diversi compiti affidati al RPD, l'art. 39, par. 1, lett. b), del RGPD riconosce al RPD il compito di sorvegliare l'osservanza del Regolamento. Il titolare del trattamento o il responsabile del trattamento, secondo il considerando 97, dovrebbe essere assistito dal RPD nel controllo del rispetto a livello interno del Regolamento.

In particolare, tra i compiti di controllo svolti dal RPD rientrano: la raccolta di informazioni per individuare i trattamenti svolti; l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Sul punto, le Linee guida del Gruppo Art. 29 fanno giustamente rilevare che "Il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza. Il RGPD chiarisce che spetta al titolare, e non al RPD, "mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento" (articolo 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD".

Il RPD svolge un ruolo non secondario nella gestione della valutazione di impatto di cui all'art. 35 del RGPD. Tuttavia, appare opportuno sottolineare che, ai sensi dell'art. 35, par. 1, spetta al titolare del trattamento, e non al RPD, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati[22]. Il RPD svolge, però, un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di detta valutazione. In applicazione del principio di data protection by design, l'art. 35, par. 2, prevede

[22] Sul punto si rinvia alle Linee-guida del Gruppo Art. 29 concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 – WP248adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 (http://ec.europa.eu/newsroom/article29/item-detailegge cfm?item_id=611236).

espressamente che il titolare si consulti con il RPD quando svolge una valutazione di impatto. L'art. 39, par. 1, lett. c), del RGPD affida al RPD il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35". Il Gruppo Art. 29 raccomanda che il titolare del trattamento si consulti con il RPD, fra l'altro, sulle seguenti tematiche: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate; se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD. Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

Il titolare del trattamento deve definire con chiarezza (per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa) i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della valutazione di impatto.

Il RPD deve cooperare con l'autorità di controllo e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione" (art. 39, par. 1, lett. d ed e). Detti compiti rientrano nel ruolo di "facilitatore" attribuito al RPD, questi funge anche da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti riconosciutele dall'art. 57 del RGPD e ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi previsti all'art. 58 del RGPD. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'art. 39, par. 1, prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

L'art. 30 del RGPD prevede che il titolare del trattamento o il responsabile del trattamento debbano tenere un registro delle attività di trattamento svolte sotto la propria responsabilità ovvero un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento. "Nella realtà, sono spesso i RPD a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE". Detto registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento. "In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'articolo 30 deve essere considerato anche uno strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione".

Come messo in luce da Antonello Soro[23], ex Presidente del Garante per la protezione dei dati personali, il protagonista della "rivoluzione" innescata dal RGPD è, accanto al titolare, proprio il RPD: figura da cui dipende la "scommessa" dell'*accountability*, la capacità cioè di fare della protezione dati non tanto un onere legale da assolvere quanto un elemento di vantaggio competitivo su cui puntare per reggere alle sfide di un mercato sempre più fondato sui dati, dei quali è quindi indispensabile assicurare protezione, qualità,

[23] Sul punto l'intervento di Antonello Soro, ex Presidente dell'Autorità Garante per la protezione dei dati personali, in occasione della piena applicazione del Regolamento (UE) 2016/679, 25 maggio 2018, Protezione dei dati: garanzia di libertà nella società digitale.

esattezza, sicurezza.

6. *Accesso a documenti amministrativi e protezione dei dati personali*

"La conoscenza ci dà potere", "sapere ci aiuta a decidere", "conoscere ci libera", è il 3 febbraio 2019 e la voce narrante dell'attore Tom Hanks declama le tre frasi chiave dello spot andato in onda durante la finale del campionato di football americano, uno spot commissionato dal Washington Post. "La democrazia muore nell'oscurità" è lo slogan finale, lo stesso che costituisce il motto del giornale che illuminò i Pentagon Papers sulla guerra in Vietnam e lo scandalo Watergate. Il terzo millennio ci ha portato anche in dote un'informazione self-made, tutta fondata sui social e sulle condivisioni, ingenerando il grande e pericoloso equivoco che non occorra autorevolezza per raccontare la realtà. Troppo spesso la quantità dell'informazione uccide la qualità e la breaking news a tutti i costi, tipiche dei siti web, appiattisce lo spessore dei fatti e nega loro complessità. I cittadini hanno bisogno di informazioni di qualità e di trasparenza al fine di attivare reali meccanismi di partecipazione democratica.

La trasparenza è uno dei miti assoluti dei nostri tempi, un tema articolato, complesso e scivoloso. In questa sezione, il tema sarà analizzato sotto il profilo più squisitamente giuridico della trasparenza dell'amministrazione pubblica, tralasciando gli aspetti filosofici e sociologici.

Gli strumenti di realizzazione del principio di trasparenza sono diversi. Alcuni di essi sono individuati nelle disposizioni della legge n. 241/1990, a questi si aggiungono le previsioni in materia di semplificazione del linguaggio dell'amministrazione, dirette a garantire maggiore visibilità dei contenuti dell'azione amministrativa.

Nell'ordinamento italiano, la trasparenza, e più in generale la disciplina del rapporto dialogico tra pubblica amministrazione e cittadino, è un istituto di recente introduzione, essendo stata prevista espressamente solo con la legge n. 241/1990.

Si tratta di un principio tutt'altro che statico: la trasparenza, infatti, costituisce uno dei gangli del diritto pubblico maggiormente soggetto all'evoluzione politica, sociale e tecnologica.

Il concetto di trasparenza nell'ordinamento giuridico italiano, nel corso degli anni, è stato legato al processo di semplificazione amministrativa, alla maggiore partecipazione dei cittadini ai processi decisionali, a una maggiore democratizzazione del rapporto tra cittadino e amministrazione per il miglioramento di quest'ultima, in particolare sotto i profili dell'efficienza e dell'imparzialità.

Il tema della trasparenza si lega a quello, come già rilevato, della semplificazione amministrativa, "La semplificazione dell'ordinamento è un compito che presenta gravissime difficoltà; ed è inutile cercare di superarle se non si hanno delle idee chiare. Insomma, bisogna sapersi orientare, anzi che procedere a tentoni"[24]. Oggi un dato certo è che per orientarsi nel semplificare occorre definire obiettivi, potenziali criticità, soggetti coinvolti, ricadute. Semplificare vuol dire attivare un processo di riforma della normativa esistente, ma anche di formazione di nuove regole, basato su dati empirici e sul coinvolgimento di tutti i soggetti interessati. "Le semplificazioni vanno anche programmate nel tempo, in modo da bilanciare adeguatamente gli sforzi in funzione di priorità condivise e raggiungibili"[25].

Con la legge 7 agosto 1990, n. 241, la semplificazione amministrativa assurge a principio generale dell'azione amministrativa, ma a quasi trent'anni dall'affermarsi di una specie di "dittatura culturale della semplificazione"[26], per usare le parole di Michele Ainis, i risultati appaiono deludenti[27]. In tale quadro, la trasparenza amministrativa diventa anch'essa un principio generale dell'attività e dell'organizzazione della

[24] F. Carnelutti, *Certezza, autonomia, libertà, diritto*, in *Il diritto dell'economia*, 1956, 1193.
[25] N. Rangone, *Semplificazione amministrativa*, in *Enciclopedia italiana Treccani*, IX Appendice, 2015, su *www.treccani.it/enciclopedia/semplificazione-amministrativa_%28Enciclopedia-Italiana%29/*
[26] M. Ainis, *La semplificazione complicante*, in *Federalismi.it*, 2014, 18, 2-9.
[27] Si vedano sul punto le conclusioni di un'indagine conoscitiva sulla semplificazione che descrivono un Paese «auto-avviluppato in una miriade di lacci e lacciuoli» (Commissione parlamentare per la semplificazione, Indagine conoscitiva sulla semplificazione legislativa ed amministrativa, nr. 32, 2014, 34, 38-39). Questa analisi, nel mettere in evidenza che la complicazione dell'ordinamento giuridico costituisce un frequente esito paradossale della semplificazione, ne fa anche emergere il carattere insostenibile in tempo di crisi. Viene poi evidenziato quanto sottolineato in dottrina e al centro del dibattito politico: una normativa inadeguata, sovrabbondante, poco comprensibile è terreno fertile per la diffusione della corruzione.

pubblica amministrazione, secondo il quale la PA è tenuta ad assicurare la visibilità, la conoscibilità e la comprensibilità della propria azione e dei propri assetti strutturali con i quali opera nel perseguire la cura in concreto dell'interesse pubblico. Principio fondamentale, questo, per l'attuazione del principio democratico nella PA, poiché coessenziale alla configurazione della democrazia come "regime del potere visibile"[28].

Il concetto di trasparenza si arricchisce di ulteriori contenuti e significati con il D.lgs. 27 ottobre 2009, n. 150 (*Ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*), che, all'art. 11, definisce la trasparenza come "accessibilità totale", da garantire essenzialmente attraverso la pubblicazione sui siti istituzionali di tutte le informazioni riguardanti ogni aspetto dell'organizzazione: "La trasparenza è intesa come accessibilità totale, anche attraverso lo strumento della pubblicazione sui siti istituzionali delle amministrazioni pubbliche, delle informazioni concernenti ogni aspetto dell'organizzazione, degli indicatori relativi agli andamenti gestionali e all'utilizzo delle risorse per il perseguimento delle funzioni istituzionali, dei risultati dell'attività di misurazione e valutazione svolta dagli organi competenti, allo scopo di favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità". Essa costituisce livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche ai sensi dell'art. 117, secondo comma, lettera m), della Costituzione[29].

Si costituisce in questo modo, in capo a ciascun cittadino, una posizione giuridica qualificata ad ottenere le informazioni pubbliche, che è chiaramente diretta a favorire quel controllo generalizzato sull'operato delle amministrazioni pubbliche, espressamente escluso dalla legge 241/1990 (art. 24, c.3). La trasparenza introdotta dal D.lgs. 150/2009 mira da un lato a garantire l'efficienza della pubblica amministrazione, tramite la trasparenza sulle performance dell'amministrazione e dei servizi pubblici, e, dall'altro, è finalizzata a prevenire la corruzione, mediante la trasparenza dei procedimenti e degli assetti organizzativi.

Ciò significa anche che i dati pubblicati "sono accessibili da parte di chiunque, che l'accessibilità non può essere limitata da aspetti tecnologici (*digital divide*), che l'accessibilità deve essere garantita come qualità delle informazioni secondo i principi di utilità, obiettività, integrità (nel senso di completezza) come individuati anche dal codice dell'amministrazione digitale: qualità dei dati in sé (esattezza, disponibilità, accessibilità e riservatezza); qualità dell'informazione aggregata (accessibilità,

[28] N. Bobbio, *La democrazia e il potere invisibile*, in *Rivista italiana di scienza politica*, vol. 10, 2, 1980, 181 ss.

[29] "La trasparenza totale persegue finalità nettamente diverse dall'accesso e connota un diverso modo di essere delle pubbliche amministrazioni che non può non spiegare effetti sugli assetti organizzativi specifici e sulle singole vicende dell'azione amministrativa. L'accessibilità totale è vista, in primo luogo, in funzione di servizio agli utenti e, ancora, sul versante della collettività, in funzione di controllo sociale diffuso sull'operato delle amministrazioni. A ben vedere, la trasparenza è posta in stretta correlazione con gli ambiti maggiormente significativi dell'attuale processo di riforma delle amministrazioni e, in un certo senso, può dirsi che la trasparenza costituisce il collante tra versante interno (organizzazione) e versante esterno (servizi al cittadino) della riforma. Sul piano macro, la trasparenza, come disciplinata dal legislatore del 2009, può dirsi finalizzata: a) all'efficienza, e quindi abbiamo le disposizioni sulla trasparenza della performance; b) alla prevenzione della corruzione e in generale di fenomeni di maladministration, cui si riporta in particolare la metodologia cd. della mappatura dei rischi nei procedimenti e negli assetti organizzativi; c) al miglioramento dei servizi pubblici, cui sono serventi sia la disciplina della performance organizzativa sia l'adozione di standard qualitativi e quantitativi nella logica del "miglioramento continuo" delle prestazioni; d) alla responsabilizzazione delle pubbliche amministrazioni, che ispira i sistemi di misurazione e valutazione. Se la trasparenza, nel contesto specifico della riforma complessiva delle amministrazioni delineata dal D.lgs. n. 150, ha queste finalità, ne discendono subito alcuni corollari che potremmo definire di sistema. Se è vero che. in presenza di una idonea base normativa, occorre tendenzialmente pubblicare tutto, è importante evitare quelle che sono state definite forme di opacità per confusione, in cui la massa di dati resi pubblici, in particolare sugli assetti organizzativi, rende impossibile l'identificazione dei dati rilevanti cioè dei dati che veramente interessano i cittadini come tali e come utenti dei servizi. L'identificazione dei dati rilevanti avviene essenzialmente attraverso i momenti di ascolto con i cittadini e le loro rappresentanze: questi momenti esprimono una "domanda di trasparenza" che va al di là della stessa "offerta di trasparenza" imposta dalla legge, perché seleziona tra i dati potenzialmente pubblici quelli di reale interesse e impone alle amministrazioni realmente aperte di concentrarsi su quelle informazioni che riguardano direttamente l'erogazione dei servizi anche al fine di assumere, nel momento della definizione degli obiettivi soprattutto di outcome. scelte coerenti con i bisogni della collettività" (F. Patroni Griffi, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *www.federalismi.it*, 2013).

elevata usabilità, interoperabilità, completezza delle informazioni, chiarezza di linguaggio, reperibilità, affidabilità, affidabilità, semplicità di consultazione, qualità, omogeneità, conformità ai documenti originali"[30].

Il D.lgs. 150/2009 prevede anche di dare pubblicità a ogni aspetto organizzativo. Nella nozione di organizzazione rientrerebbero sia l'elemento oggettivo (le funzioni di attività predeterminate in vista della cura di finalità di interesse generale, funzioni scopo), le competenze, i caratteri degli organi, le discipline sul funzionamento degli organi, le tipologie dei procedimenti, sia l'elemento soggettivo (il titolare dell'organo, il responsabile del procedimento, il personale addetto, le informazioni personali rilevanti).

Nonostante la piena operatività del RGPD e le conseguenti modifiche apportate dal legislatore al Codice in materia di protezione dei dati personali, la disciplina dell'accesso ai documenti amministrativi, disciplinato dalla legge 7 agosto 1990, n. 241[31], è rimasto inalterato. All'art. 59 del Codice è sempre presente una clausola di salvezza in base alla quale restano ferme le disposizioni della legge n. 241/1990, dei successivi regolamenti di attuazione e delle altre leggi regolanti il diritto di accesso: "Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso". Sempre l'art. 59 del Codice precisa che i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal d.lgs. 14 marzo 2013, n. 33.

L'articolo successivo evidenzia che "Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale".

La legge n. 241 del 1990, come già rilevato, per prima ha riconosciuto il diritto di accesso agli atti della pubblica amministrazione. Occorre che tale diritto sia assicurato a chiunque vi abbia interesse, il legislatore non ha tuttavia contemplato un'azione popolare volta a consentire un controllo generalizzato sull'attività amministrativa. E infatti, la norma correla espressamente l'interesse all'ostensione alla tutela di situazioni giuridicamente rilevanti: l'art. 22, comma 1, lett. b) della legge n. 241 del 1990, infatti, definisce "interessati" all'accesso non già tutti i soggetti indiscriminatamente, ma esclusivamente i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso[32].

La legge ha avuto il merito di aprire le porte ai cittadini nei confronti di un sistema che, fino a quel momento, aveva visto affermarsi la superiorità della pubblica amministrazione sugli stessi e che si esplicava nell'assoluta riservatezza dei procedimenti amministrativi. Questo sistema è stato scardinato dalla citata legge, voluta non solo per avvicinare il modus operandi della pubblica amministrazione a quello delle altre legislazioni europee, ma anche per renderlo più affine al dettato costituzionale che, all'art. 97, individua nel buon andamento e nell'imparzialità i principi cardine cui la pubblica amministrazione italiana dovrebbe uniformarsi.

Anche se questa legge è stata fondamentale per avviare quello che è stato in un certo senso un cambiamento dei paradigmi del rapporto tra pubblica amministrazione e cittadini, occorre, però, rimarcare che si parla pur sempre di accesso documentale, ciò significa che non è un accesso consentito a tutti e in qualsiasi momento, ma solo a determinate

[30] F. Merloni e B. Ponti, *Gli strumenti della trasparenza*, in F. Merloni, L. Vandelli (a cura di), *La corruzione amministrativa*, Firenze, Passigli Editori, 2010, 410-411.

[31] In questa sede, appare pleonastico soffermarsi sull'annosa questione del rapporto tra accesso ai documenti amministrativi e tutela della riservatezza, tema rispetto al quale, da tempo, sono stati spesi fiumi d'inchiostro.

[32] Cons. Stato, sez. V, 21 agosto 2017, n. 4043.

condizioni: ovvero ci deve essere un interesse diretto, concreto e attuale che faccia riferimento ad una situazione giuridica tutelata dall'ordinamento e collegata ai documenti per i quali si richiede l'accesso, come recita lo stesso art. 22, comma 1. Proseguendo nella sommaria analisi della legge n. 241/90, non si può non segnalare quello che è il vero fulcro dell'accesso agli atti documentale, cioè la possibilità di prendere visione degli stessi. Difatti, grazie all'art. 22, comma 2, è possibile prendere visione degli atti ed estrarne copia, cosa impensabile fino a qualche anno fa e segno inequivocabile che i rapporti di forza tra cittadini e pubblica amministrazione stavano inevitabilmente cambiando.

Se da un lato ci sono aspetti positivi, dall'altro bisogna sottolineare che non è una legge libera tutti: infatti, sono ancora presenti segni tangibili di quella diffidenza che ha caratterizzato, e che caratterizza tutt'ora, il rapporto tra pubblica amministrazione e cittadini.

L'art. 24, comma 1, regola proprio i casi di esclusione all'accesso, come: i documenti coperti dal segreto di Stato, i procedimenti tributari, gli atti normativi ed amministrativi generali; casi che per nostra sfortuna non sono pochi. Tra l'altro il dettato dell'art. 24, comma 6, della citata legge, prevede come il governo possa ulteriormente rafforzare i limiti all'accesso nel caso in cui i documenti amministrativi dovessero riguardare argomenti sensibili quali: la sicurezza nazionale e la difesa nazionale; l'eventuale danno ai processi di formazione e attuazione della politica monetaria; il potenziale danno alla vita privata di persone fisiche, persone giuridiche, enti. L'ultimo comma dell'art. 24 sembra quasi contemplare un piccolo risarcimento: infatti, il legislatore ha concesso l'accesso ai documenti amministrativi in caso di difesa dei propri interessi giuridici e, se dovessero esserci in ballo dati sensibili e giudiziari, il suddetto accesso è consentito nei limiti strettamente previsti.

7. *Accesso civico "semplice", accesso "generalizzato" e protezione dei dati personali*

La democrazia è idealmente il governo del potere visibile, cioè del governo i cui atti si svolgono in pubblico, sotto il controllo della pubblica opinione. Le istituzioni di un paese libero non possono durare a lungo, scrisse nel secolo scorso Maurice Joly nel suo *Dialogo agli inferi* tra Machiavelli e Montesquieu[33], se non agiscono *au grand jour* (alla luce del sole).

Tema ricorrente della dottrina dello Stato assoluto è quello degli *arcana imperii*. Uno dei più noti scrittori machiavellici, Gabriel Naudé, ha sentenziato: "Non vi è nessun principe così debole e privo di senno da essere scriteriato al punto da rimettere al giudizio del pubblico ciò che a mala pena rimane segreto se confidato all'orecchio di un ministro o di un favorito"[34]. Il potere autocratico si sottrae al controllo del pubblico in due modi: occultandosi, cioè prendendo le proprie decisioni nel «consiglio segreto», e occultando, cioè attraverso l'esercizio della simulazione o della menzogna considerata come lecito strumento di governo.

"Il segreto sta nel nucleo più interno del potere". Norberto Bobbio usava spesso citare questo passo di *Massa e potere* di Elias Canetti per sottolineare come, per secoli, il segreto sia stato considerato da uomini di Stato e teorici della politica uno strumento essenziale all'esercizio del potere.

A questa teoria (e pratica) degli *arcana imperii* i sostenitori della democrazia hanno contrapposto l'idea di un potere "in pubblico", in cui, kantianamente, si faccia un «uso pubblico della ragione», cioè si discuta in modo informato e competente sui problemi della comunità per giungere a decisioni consapevoli e condivise e per esercitare un efficace controllo sui governanti.

Peraltro un simile obiettivo non è stato raggiunto a giudizio di Bobbio, che nel saggio *II futuro della democrazia* indica nell'eliminazione del potere invisibile una delle sei grandi promesse non mantenute dall'ideologia democratica[35].

Colin Crouch[36], sociologo e politologo britannico, è noto per aver coniato il termine post-democrazia. Ossia una condizione in cui la pratica democratica perde di consistenza, garantendo solo libertà svuotate di contenuto. La politica smarrisce il contatto con i cittadini.

"Chi guardi il generale processo di riforme, che hanno interessato l'amministrazione

[33] M. Joly, *Dialogo agli inferi tra Machiavelli e Montesquieu*, Genova, ECIG, 1995.
[34] In N. Bobbio, *La democrazia e il potere invisibile*, 191.
[35] N. Bobbio, *Il futuro della democrazia*, Torino, Einaudi, 1984.
[36] C. Crouch, *Postdemocrazia*, Roma-Bari, Laterza, 2000.

pubblica quanto meno a partire dagli anni '90, noterà l'emersione progressiva nel mondo del diritto di quello che potremmo definire un valore dell'ordinamento che a poco a poco acquisterà contorni sempre più netti e pervasivi della tradizionale sfera di "riservatezza" delle pubbliche amministrazioni, nell'ottica di un dialogo tra amministrazione e amministrato che favorisca la trasformazione del suddito in cittadino (l'immagine è mutuata dal prezioso saggio di W. Ulmann, su *Individuo e società nel Medioevo*, edito da Laterza nel 1983).

Da allora la trasparenza assumerà sempre più le sembianze di un valore immanente all'ordinamento, un valore di tipo finalistico, perché espressione di democrazia politica e amministrativa; ma anche un valore strumentale, e quindi formale, attraverso il quale assicurare la conoscenza dei processi decisionali, delle organizzazioni, dei procedimenti, delle prestazioni e dei servizi al pubblico.

Volendo schematizzare il percorso normativo registratosi, è consentito tener conto di tre tappe evolutive:

a. quella inaugurata con l'approvazione della legge n. 241 del 1990;

b. quella che ha inizio con l'affermazione, ad opera del D.lgs. n. 150 del 2009, del principio di accessibilità totale;

c. quella, infine, che prende avvio con il D.lgs.14 marzo 2013, n. 33, recante "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione" e adottata in attuazione della delega contenuta nella legge 6 novembre 2012, n. 190 (legge c.d. anticorruzione)"[37], che si arricchisce di un più articolato e complesso strumento di accesso introdotto con il D.lgs. n. 97/2016: l'accesso c.d. generalizzato.

Con la legge n. 190/2012 la trasparenza diventa uno dei principali strumenti di contrasto e prevenzione della corruzione, alla luce del D.lgs. n. 33/2013, che mira a rendere accessibili non solo le azioni cristalizzate negli atti, ma anche le condizioni personali del soggetto che le pone in essere.

Dopo l'introduzione dell'informatica nell'attività amministrativa e il ripensamento sul ruolo del settore pubblico, l'originario concetto di trasparenza (circoscritto al diritto di accesso agli atti e ai documenti per coloro che avessero specifico e concreto interesse) ha iniziato a dimostrarsi insufficiente. La digitalizzazione della PA conferisce nuovi significati al concetto di trasparenza (si pensi agli artt. 2, 12 e 50 del CAD).

Il tema dell'amministrazione aperta, e dei suoi principi, si lega strettamente ad una riflessione sull'amministrazione elettronica, specie se letta da un'angolazione attenta ai diritti del cittadino. Il Codice dell'amministrazione digitale, che disciplinando la presenza nel web delle pubbliche amministrazioni ha posto le premesse per la successiva maturazione di un nuovo modello di trasparenza attraverso la diffusione di informazioni tramite siti istituzionali, sul quale ultimo il legislatore ha puntato con forza a partire dalle riforme del 2009 per arrivare al decreto legislativo n. 33 del 2013, riformato nel corso del 2016.

Di questo stretto collegamento tiene conto il legislatore: così, recentemente, di amministrazione "digitale ed aperta" si occupa la legge c.d. Madia n. 124/2015, art. 1, lett. n), che collega i due concetti quasi come endiadi: la riorganizzazione delle amministrazioni sul versante dell'informatizzazione è finalizzata "alla realizzazione di un'amministrazione digitale e aperta", oltre che di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

Parlare di "openness" significa, in questo scenario, segnare la "mutazione genetica" che ha interessato la trasparenza, come principio e negli strumenti chiamata a realizzarlo: nel corso degli ultimi anni si è assistito ad un forte cambiamento di prospettiva, con la perdita di centralità del diritto di accesso in favore della trasparenza assicurata dalla pubblicazione nei siti istituzionali e quindi della disponibilità (on line) di informazioni: né il percorso di evoluzione sembra arrestato, posto che il legislatore ha nel 2016 introdotto una disciplina ispirata al modello del Freedom of Information Act. Uno sviluppo che ci consegna un quadro composito di strumenti della trasparenza, sempre meno collegabile a meccanismi di garanzia del singolo interessato, ma sempre più declinata in termini di autonomo diritto alla conoscibilità.

Tutto deve essere accessibile, tutto deve essere visibile. La trasparenza viene istituzionalizzata, questa si condensa nell'imperativo di svelare ciò che è nascosto e non stupisce il fatto che sia assurta a

[37] F. Patroni Griffi, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *Federalismi.it*, 2013.

condizione della democrazia. Nel mondo anglosassone il cardine della democrazia è l'*accountability*, "il dovere di rendere conto". Ma se il controllo diffuso, pubblico, è il fermento del dissenso, equiparare "pubblico" a "democratico", in una visione manichea e ingenua, può portare a storture inquietanti. "Muoversi nel diafano palazzo di cristallo non è poi così semplice. Si rischia di urtare contro le pareti invisibili, la trasparenza inganna. Il sogno diventa un incubo". Anche coloro che credono fideisticamente nell'altissimo cielo della trasparenza, come ricorda Vladimir Nabokov in "Cose trasparenti"[38] , prima o poi saranno costretti ad ammettere che questa non è che un abbaglio e vano sarebbe rincorrere l'ideale della trasparenza assoluta[39] .

Anche la trasparenza e la luce devono essere sottoposte alla nostra capacità critica, come scriveva Hegel, "nell'assoluta chiarezza non ci si vede né più né meno che nell'assoluta oscurità". Questa affermazione, oggi, si rivela in tutta la sua attualità. "Oggi, infatti, viviamo in un mondo ad altissima visibilità in cui però molto resta celato agli occhi della coscienza. La grande quantità di immagini e di dati a nostra disposizione ci permettono di vedere posti remoti e di accedere a informazioni che fino a tempi recenti erano privilegio di pochi. Ciò non implica, però, necessariamente un miglioramento della nostra capacità di analisi e conoscenza. Ci sentiamo spesso accecati; vediamo ma non sempre capiamo. Ci illudiamo che la rapidità della comunicazione ci mostri immediatamente il reale, ma dimentichiamo che vecchi e nuovi media continuano a selezionare, scegliere, mediare. Inoltre, le nostre vite sono continuamente sotto i riflettori, e come attori su un palcoscenico siamo in mostra senza vedere il pubblico, abbagliati da troppa luce. La trasparenza, certo, è necessaria al governo democratico, da sempre legittimato proprio dalla possibilità per i cittadini di vedere all'opera i propri rappresentanti sul palcoscenico della politica… Perché rinnovare la società democratica vuol dire riaprire canali di dialogo fra rappresentanti e rappresentati ma soprattutto fra cittadini; rinnovare lo scambio fra persone differenti e mondi tra loro lontani. Tra cultura umanistica e scientifica, tra centro e periferia, tra alto e basso, per superare la logica di contrapposizione che riduce la politica ad un campo di battaglia in cui si affrontano nemici. Per quanto faticoso tutto ciò possa apparire, questo è il terreno su cui si gioca la sopravvivenza della democrazia" [40].

Come già rilevato, con il d.lgs.14 marzo 2013 n. 33, intitolato "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" il legislatore – in attuazione della delega contenuta nella legge 6 novembre 2012, n. 190, recante: "Disposizioni per la prevenzione e la repressione della corruzione e dell´illegalità nella pubblica amministrazione" (art. 1, commi 35 e 36) – ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzione di dati, informazioni, atti e documenti sui siti web istituzionali dei soggetti obbligati. A tal fine, nel capo I dedicato ai "principi generali", la trasparenza è definita come "come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche" (art. 1, comma 1).

Nel medesimo capo I è precisato che "oggetto del decreto" è quello di disciplinare "la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione". Si sottolinea, in proposito, che lo stesso legislatore, ai soli fini del campo di applicazione del decreto, definisce la pubblicazione come la diffusione "in conformità alle specifiche e alle regole tecniche di cui all'allegato A, nei siti

[38] V. Nabokov, *Cose trasparenti*, Milano, Adelphi, 1995.

[39] G. Greenwald, *No place to hide. Sotto controllo, Edward Snowden e la sorveglianza di massa*, Milano, Rizzoli, 2014.

[40] G. Zagrebelsky, *Luci, oscurità e nuovi poteri nella società della vetrina*, in *La Repubblica*, 20 marzo 2019, 33.

istituzionali delle pubbliche amministrazioni dei documenti, delle informazioni e dei dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, cui corrisponde il diritto di chiunque di accedere ai siti direttamente ed immediatamente, senza autenticazione ed identificazione. (art. 2, comma 2). Da ciò si evince che tutte le volte in cui nel d.lgs. n. 33/2013 è utilizzata la locuzione "pubblicazione obbligatoria ai sensi della normativa vigente", il riferimento è limitato agli "obblighi di pubblicazione concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" contenuti oltre che nel d.lgs. n. 33/2013 anche in altre disposizioni normative aventi analoga finalità di trasparenza, con esclusione degli obblighi di pubblicazione aventi finalità diverse.

La tipologia dei predetti obblighi di pubblicazione per finalità di trasparenza concernenti l´organizzazione e l´attività delle pubbliche amministrazioni è schematicamente riassunta nell´allegato A al d.lgs. n. 33/2013 che individua la "struttura delle informazioni sui siti istituzionali"(1) e che precisa come la sezione dei siti istituzionali denominata "Amministrazione trasparente" deve essere organizzata in sotto-sezioni all´interno delle quali devono essere inseriti i documenti, le informazioni e i dati previsti dal decreto.

Devono, pertanto, ritenersi estranei all'oggetto del d.lgs. n. 33/2013 tutti gli obblighi di pubblicazione previsti da altre disposizioni per finalità diverse da quelle di trasparenza, quali gli obblighi di pubblicazione a fini di pubblicità legale, pubblicità integrativa dell'efficacia, pubblicità dichiarativa o notizia. Si pensi, ad esempio – tra i diversi casi indicati – alle pubblicazioni matrimoniali, la cui affissione alla porta della casa comunale (e oggi sui siti web istituzionali dei comuni) è prevista per otto giorni (cfr. art. 55 del d.P.R. n. 396 del 3/11/2000). La pubblicazione dei dati personali dei nubendi assolve a una funzione che evidentemente esula dalle finalità di trasparenza previste dal d.lgs. n. 33/2013 e che è pienamente assolta con la semplice pubblicazione per la durata temporale prevista. Infatti, sarebbe irragionevole applicare a essi il regime di conoscibilità previsto dalla normativa sulla trasparenza (limiti temporali di permanenza sul web, indicizzazione, accesso civico, riutilizzo etc.). Pertanto, tutte le ipotesi di pubblicità non riconducibili a finalità di trasparenza, qualora comportino una diffusione di dati personali, sono escluse dall'oggetto del d.lgs. n. 33/2013 e dall´ambito di applicazione delle relative previsioni fra cui, in particolare, quelle relative all´accesso civico (art. 5), all´indicizzazione (art. 4 e 9), al riutilizzo (art. 7), alla durata dell´obbligo di pubblicazione (art. 8) e alla trasposizione dei dati in archivio (art. 9).

Il Garante per la protezione dei dati personali, al fine di garantire i diritti e le libertà fondamentali (con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali) e contribuire a declinare in modo equilibrato il rapporto tra esigenze di trasparenza dell'amministrazione e garanzie poste a tutela dei diritti, il 15 maggio 2014 ha, a proposito, adottato delle linee guida, alla ricerca di un corretto bilanciamento, di un ragionevole equilibrio, tra attuazione del principio di trasparenza e tutela dei dati personali.

Infatti, i principi e la disciplina di protezione dei dati personali (come peraltro previsto anche dagli artt. 1, comma 2, e 4 del d.lgs. n. 33/2013; v. altresì art. 8, comma 3) devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.

La "diffusione" di dati personali – ossia "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione" (art. 4, comma 1, lett. m) – da parte dei "soggetti pubblici" è ammessa unicamente quando la stessa è prevista da una specifica norma di legge o di regolamento. Pertanto, in relazione all'operazione di diffusione, occorre che le pubbliche amministrazioni, prima di mettere a disposizione sui propri siti web istituzionali informazioni, atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, verifichino che la normativa in materia di trasparenza preveda tale obbligo. Qualora l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell´atto o del documento nel proprio sito web istituzionale è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l´oscuramento di determinate informazioni. I soggetti pubblici, infatti, in conformità ai principi di protezione

dei dati, sono tenuti a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l´interessato solo in caso di necessità (cd. "principio di minimizzazione o necessità"). Pertanto, anche in presenza degli obblighi di pubblicazione di atti o documenti contenuti nel d.lgs. n. 33/2013, i soggetti chiamati a darvi attuazione non possono comunque rendere intelligibili i dati personali non pertinenti o, se particolari o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione. È, quindi, consentita la diffusione online dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti. È, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" e "la vita sessuale" (art. 4, comma 6, del d.lgs. n. 33/2013).

In particolare, con riferimento ai dati idonei a rivelare lo stato di salute degli interessati, è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Il procedimento di selezione dei dati personali che possono essere resi conoscibili online deve essere, inoltre, particolarmente accurato nei casi in cui tali informazioni siano idonee a rivelare l´origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l´adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale ("dati particolari"), oppure nel caso di dati idonei a rivelare provvedimenti di cui all´articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, nonché la qualità di imputato o di indagato ("dati giudiziari").

I dati particolari e giudiziari, infatti, sono protetti da un quadro di garanzie particolarmente stringente che prevede la possibilità per i soggetti pubblici di diffondere tali informazioni solo nel caso in cui sia previsto da una espressa disposizione di legge e di trattarle solo nel caso in cui siano in concreto "indispensabili" per il perseguimento di una finalità di rilevante interesse pubblico come quella di trasparenza; ossia quando la stessa non può essere conseguita, caso per caso, mediante l´utilizzo di dati anonimi o di dati personali di natura diversa. Pertanto, come rappresentato dal Garante per la protezione dei dati personali nel parere del 7 febbraio 2013 (doc. web 2243168), gli enti pubblici sono tenuti a porre in essere la massima attenzione nella selezione dei dati personali da utilizzare, sin dalla fase di redazione degli atti e documenti soggetti a pubblicazione, in particolare quando vengano in considerazione dati sensibili. In proposito, può risultare utile non riportare queste informazioni nel testo dei provvedimenti pubblicati online (ad esempio nell´oggetto, nel contenuto, etc.), menzionandole solo negli atti a disposizione degli uffici (richiamati quale presupposto del provvedimento e consultabili solo da interessati e controinteressati), oppure indicare delicate situazioni di disagio personale solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici (cfr. par. 2 del parere citato).

Una volta effettuata la preventiva valutazione circa i presupposti e l´indispensabilità della pubblicazione di dati sensibili e giudiziari, devono essere adottate idonee misure e accorgimenti tecnici volti ad evitare "la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo" (cfr. art. 7, del d.lgs.n. 33/2013, nonché le precisazioni fornite dal Garante nel parere sopra richiamato).

L´art. 6 del d.lgs. n. 33/2013 prevede che "Le pubbliche amministrazioni garantiscono la qualità delle informazioni riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti dalla legge, assicurandone l´integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l´omogeneità, la facile accessibilità, nonché la conformità ai

documenti originali in possesso dell´amministrazione, l´indicazione della loro provenienza e la riutilizzabilità secondo quanto previsto dall´art. 7"[41] e che "l´esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l´omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti".

Tale previsione deve essere interpretata anche alla luce dei principi in materia di protezione dei dati personali, per cui le pubbliche amministrazioni sono, altresì, tenute a mettere a disposizione soltanto dati personali esatti, aggiornati e contestualizzati. Le pubbliche amministrazioni titolari del trattamento devono, quindi, non solo controllare l´attualità delle informazioni pubblicate, ma anche modificarle o aggiornarle opportunamente, quando sia necessario all´esito di tale controllo e ogni volta che l´interessato ne richieda l´aggiornamento, la rettificazione oppure, quando vi abbia interesse, l´integrazione. Ormai siamo entrati in una seconda fase. Occorre passare dall'elemento puramente quantitativo a quello qualitativo. L'accumulo di informazioni non produce di per sé verità e trasparenza e non genera di per sé nuova conoscenza. Più informazioni non eliminano la fondamentale opacità del tutto, anzi rischiano di accrescerla. L'iperinformazione spesso non getta alcuna luce nelle tenebre. Esiste, infatti, la c.d. opacità per confusione. È il tema del *civic engagement*: provare a coinvolgere i cittadini per risolvere problemi comuni. Nell'adempimento degli obblighi di pubblicazione deve essere garantita la qualità dei dati, assicurandone il costante e tempestivo aggiornamento, la "comprensibilità", la "completezza", "l'integrità" e "l'omogeneità", nonché la conformità agli originali in possesso del soggetto obbligato alla pubblicazione, l'indicazione della provenienza e deve essere eliminato ogni ostacolo e difficoltà all'accessibilità e alla consultazione. È espressamente previsto, inoltre, che l'esigenza di garantire la qualità dei dati non possa giustificare l'omissione o il ritardo nell'adempimento degli obblighi di pubblicazione.

La necessità di assicurare una qualità adeguata dei dati pubblicati è funzionale all'effettività del controllo diffuso della cittadinanza che le norme in esame mirano a garantire e la relativa disciplina si completa con i rimedi previsti a fronte dell'inerzia del soggetto pubblico, ma anche dall'ulteriore obbligo delle amministrazioni pubbliche di garantire la qualità delle informazioni pubblicate.

È dunque necessario garantire l'adeguata qualità delle informazioni mediante la semplicità nella accessibilità e nella consultazione dei dati, la comprensibilità delle informazioni e il loro diligente e tempestivo aggiornamento; standards che i nuovi strumenti tecnologici possono concorrere ad assicurare. La trasparenza vede infatti come necessario corollario la "comprensione" dei dati, superando le barriere che su un piano organizzativo limitano l'individuazione delle informazioni utili al controllo democratico.

La problematica della qualità delle informazioni è in grado di influire in modo significativo sulle modalità di azione e di relazione delle amministrazioni pubbliche, ma è anche una sfida difficilmente eludibile, se è vero che l'esigenza di disporre di informazioni caratterizzate da uno specifico regime di qualità attesa, è sempre più sentita a livello di organizzazioni complesse. In via generale, possiamo definire la qualità dei dati come "l'insieme delle caratteristiche di un'entità, idonee a soddisfare le esigenze esplicite ed implicite, e questa risulta centrale per garantire l'efficienza delle condotte degli operatori, per ridurre i costi ed aumentare la soddisfazione degli utenti clienti, per consentire la comunicazione tra strutture diverse, per permettere l'assunzione di decisioni corrette"[42].

L´art. 7 del d.lgs. n. 33/2013 prevede che "I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, resi disponibili anche a seguito dell´accesso civico di cui all´articolo 5, sono pubblicati in formato di tipo aperto ai sensi dell´articolo 68 del Codice dell'am-

[41] E. Carloni, *La qualità delle informazioni pubbliche. L'esperienza italiana nella prospettiva comparata*, in *Rivista trimestrale di diritto pubblico*., 2009, 155; F. Di Mascio, *Open data e trasparenza in Italia: quantità senza qualità*, in A. Natalini e G. Vesperini (a cura di), *Il Big Bang della trasparenza*, Napoli, Editoriale Scientifica, 2015, 275.

[42] E. Carloni, *La qualità delle informazioni pubbliche. L'esperienza italiana nella prospettiva comparata*, in *Riv. trim. dir. pub.*, 155. Sulla qualità delle informazioni pubbliche, cfr. anche F. Di Mascio, *Open data e trasparenza in Italia: quantità senza qualità*, 275.

ministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e sono riutilizzabili ai sensi del decreto legislativo 24 gennaio 2006, n. 36, del decreto legislativo 7 marzo 2005, n. 82, e del decreto legislativo 30 giugno 2003, n. 196, senza ulteriori restrizioni diverse dall´obbligo di citare la fonte e di rispettarne l´integrità". Detta disposizione persegue, peraltro, lo scopo di non obbligare gli utenti a dotarsi di programmi proprietari o a pagamento per la fruizione – e, quindi, per la visualizzazione – dei file contenenti i dati oggetto di pubblicazione obbligatoria. Infatti, il "formato di tipo aperto" è "un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi" (art. 68, comma 3, lett. a, del d.lgs.7 marzo 2005, n. 82, Codice dell'amministrazione digitale-CAD). Con riferimento ai dati personali, si rappresenta, quindi, che l´obbligo di pubblicazione in "formato di tipo aperto" non comporta che tali dati, pubblicati sui siti web istituzionali in ottemperanza agli obblighi di trasparenza, siano anche "dati di tipo aperto" nei termini definiti dal CAD. Appare opportuno, infatti, tenere distinto il concetto di "formato di tipo aperto" avente il significato sopra descritto, da quello di "dato di tipo aperto" che attiene, invece, più propriamente alla disponibilità unita alla riutilizzabilità del dato da parte di chiunque, anche per finalità commerciali e in formato disaggregato (art. 52, comma 2, e art. 68, comma 3, lett. b, del CAD).

Gli artt. 7 e 7-*bis* del d.lgs. n. 33/2013 stabiliscono che il riutilizzo dei dati personali pubblicati è soggetto alle condizioni e ai limiti previsti dalla disciplina sulla protezione dei dati personali e dalle specifiche disposizioni del d.lgs. 24 gennaio 2006 n. 36 di recepimento della direttiva 2003/98/CE sul riutilizzo dell'informazione del settore pubblico. Tale direttiva è stata oggetto di revisione (v. direttiva 2013/37/UE entrata in vigore dopo l'approvazione del decreto legislativo sulla trasparenza). Con la modifica della predetta direttiva, l'Unione europea conferma il principio, da ritenersi ormai consolidato in ambito europeo, in base al quale il riutilizzo di tali documenti non deve pregiudicare il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali fissato dalle disposizioni di diritto europeo e nazionale in materia. In particolare, le nuove disposizioni della direttiva introducono specifiche eccezioni al riutilizzo fondate sui principi di protezione dei dati, prevedendo che una serie di documenti del settore pubblico contenenti tale tipologia di informazioni siano sottratti al riuso anche qualora siano liberamente accessibili online. Ciò significa che il principio generale del libero riutilizzo di documenti contenenti dati pubblici, stabilito dalla disciplina nazionale ed europea, riguarda essenzialmente documenti che non contengono dati personali oppure riguarda dati personali opportunamente aggregati e resi anonimi. In altri termini, il semplice fatto che informazioni personali siano rese pubblicamente conoscibili online per finalità di trasparenza non comporta che le stesse siano liberamente riutilizzabili da chiunque e per qualsiasi scopo, bensì impone al soggetto chiamato a dare attuazione agli obblighi di pubblicazione sul proprio sito web istituzionale di determinare – qualora intenda rendere i dati riutilizzabili – se, per quali finalità e secondo quali limiti e condizioni eventuali utilizzi ulteriori dei dati personali resi pubblici possano ritenersi leciti alla luce del "principio di finalità" e degli altri principi di matrice europea in materia di protezione dei dati personali.

Al fine di evitare di perdere il controllo sui dati personali pubblicati online in attuazione degli obblighi di trasparenza e di ridurre i rischi di loro usi indebiti, è quindi in primo luogo opportuno che le pubbliche amministrazioni e gli altri soggetti chiamati a dare attuazione agli obblighi di pubblicazione di cui al d.lgs. n. 33/2013 inseriscano nella sezione denominata "Amministrazione trasparente" dei propri siti web istituzionali un Alert generale con cui si informi il pubblico che i dati personali pubblicati sono "riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva comunitaria 2003/98/CE e d.lgs.36/2006 di recepimento della stessa), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali".

A tal proposito, giova ricordare che una volta effettuata la pubblicazione online dei dati personali prevista dalla normativa in materia di trasparenza, il soggetto pubblico può rendere riutilizzabili tali dati o accogliere eventuali richieste di riutilizzo degli stessi da parte di terzi, solamente dopo avere effettuato una rigorosa valutazione d´impatto in materia

di protezione dei dati, al fine di ridurre il rischio di perdere il controllo sulle medesime informazioni o di dover far fronte a richieste di risarcimento del danno da parte degli interessati.

L'art. 7-*bis* del d.lgs. n. 33/2013 prevede che: "Gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari, di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali. La pubblicazione nei siti istituzionali, in attuazione del presente decreto, di dati relativi a titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali. Le pubbliche amministrazioni possono disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non hanno l'obbligo di pubblicare ai sensi del presente decreto o sulla base di specifica previsione di legge o regolamento, nel rispetto dei limiti indicati dall'articolo 5-*bis*, procedendo alla indicazione in forma anonima dei dati personali eventualmente presenti. Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione. Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione sono rese accessibili dall'amministrazione di appartenenza. Non sono invece ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione dal lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il predetto dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di cui all'articolo 4, comma 1, lettera d), del decreto legislativo 30 giugno 2003, n. 196. Restano fermi i limiti all'accesso e alla diffusione delle informazioni di cui all'articolo 24, commi 1 e 6, della legge 7 agosto 1990, n. 241, e successive modifiche, di tutti i dati di cui all'articolo 9 del decreto legislativo 6 settembre 1989, n. 322, di quelli previsti dalla normativa europea in materia di tutela del segreto statistico e di quelli che siano espressamente qualificati come riservati dalla normativa nazionale ed europea in materia statistica, nonché quelli relativi alla diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale".

Un'altra questione di non secondaria importanza riguarda la decorrenza e la durata dell'obbligo di pubblicazione, al riguardo l'art. 8 del d.lgs. 33/2013 dispone che: "I documenti contenenti atti oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione. I documenti contenenti altre informazioni e dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati e mantenuti aggiornati ai sensi delle disposizioni del presente decreto. I dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali e quanto previsto dagli articoli 14, comma 2, e 15, comma 4. Decorsi detti termini, i relativi dati e documenti sono accessibili ai sensi dell'articolo 5. L'Autorità nazionale anticorruzione, sulla base di una valutazione del rischio corruttivo, delle esigenze di semplificazione e delle richieste di accesso, determina, anche su proposta del Garante per la protezione dei dati personali, i casi in cui la durata della pubblicazione del dato e del documento può essere inferiore a 5 anni.

Sono, però, previsti espressamente alcune deroghe alla durata temporale quinquennale: a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della

produzione degli effetti; b) per alcuni dati e informazioni riguardanti i "titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale" (art. 14, comma 2) e i "titolari di incarichi dirigenziali e di collaborazione o consulenza" che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell´incarico (art. 15, comma 4); c) nel caso in cui siano previsti "diversi termini" dalla normativa in materia di trattamento dei dati personali. In merito, si evidenzia come il Codice – che non prevede termini espliciti (come già evidenziato dal Garante nel parere del 7 febbraio 2013), – richiede espressamente che i dati personali devono essere "conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati" e che l´interessato ha diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati. Tali principi erano già declinati nella direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali le quali, in quanto tali, non possono essere derogate dalla disciplina nazionale in virtù del primato del diritto europeo. Da tale principio, inoltre, discende l´obbligo di interpretare il diritto nazionale in maniera conforme al diritto europeo e, nello specifico, alle disposizioni direttamente applicabili che impongono il rispetto dei principi di pertinenza, necessità e proporzionalità, in base alle quali la pubblicazione di dati personali è consentita soltanto quando è al contempo necessaria e appropriata rispetto all´obiettivo perseguito e, in particolare, quando l´obiettivo perseguito non può essere realizzato in modo ugualmente efficace con modalità meno pregiudizievoli per la riservatezza degli interessati".[43] Per tale motivo, il Garante ritiene che laddove atti, documenti e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, anche prima del termine di cinque anni, quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti stessi hanno prodotto i loro effetti.

Secondo l´art. 9 del d.lgs. n. 33/2013 le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente". "Si evidenzia che l´obbligo di indicizzazione nei motori generalisti durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati ai sensi delle disposizioni in materia di trasparenza da collocarsi nella "sezione "Amministrazione trasparente", con esclusione di altri dati che si ha l´obbligo di pubblicare per altre finalità di pubblicità diverse da quelle di "trasparenza"… Sono, fra l´altro, espressamente sottratti all´indicizzazione i dati sensibili e i dati giudiziari (art. 4, comma 1, d.lgs. n. 33/2013). Pertanto, i soggetti destinatari degli obblighi di pubblicazione previsti dal d.lgs. n. 33/2013 devono provvedere alla relativa deindicizzazione tramite – ad esempio – l´inserimento di *metatag noindex* e *noarchive* nelle intestazioni delle pagine web o alla codifica di regole di esclusione all´interno di uno specifico file di testo (il file robots.txt) posto sul server che ospita il sito web configurato in accordo al *Robot Exclusion Protocol* (avendo presente, comunque, come tali accorgimenti non sono immediatamente efficaci rispetto a contenuti già indicizzati da parte dei motori di ricerca Internet, la cui rimozione potrà avvenire secondo le modalità da ciascuno di questi previste)"[44].

La disciplina in materia di trasparenza prevede di rendere visibile al pubblico, rispetto a taluni soggetti, informazioni personali concernenti il percorso di studi e le esperienze professionali rilevanti, nella forma del curriculum redatto in conformità al vigente modello europeo (art. 10, comma 8, lett. d, d.lgs. n. 33/2013). Le ipotesi contemplate riguardano, ad esempio, i curricula professionali dei titolari di incarichi di indirizzo politico (art. 14), dei titolari di incarichi amministrativi di vertice, dirigenziali

[43] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, 15 maggio 2014, doc. web 3134436.

[44] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, 15 maggio 2014, doc. web 3134436.

e di collaborazione o consulenza (art. 15, comma 1, lett. b), nonché delle posizioni dirigenziali attribuite a persone – anche esterne alle pubbliche amministrazioni – individuate discrezionalmente dall´organo di indirizzo politico senza procedure pubbliche di selezione, di cui all´articolo 1, commi 39 e 40, della legge 6 novembre 2012, n. 190 (art. 15, comma 5), dei componenti degli organismi indipendenti di valutazione (art. 10, comma 8, lett. c), nonché dei dirigenti in ambito sanitario come individuati dall´art. 41, commi 2 e 3.

Il riferimento del legislatore all´obbligo di pubblicazione del curriculum non può però comportare la diffusione di tutti i contenuti astrattamente previsti dal modello europeo (rispondendo taluni di essi alle diverse esigenze di favorire l´incontro tra domanda e offerta di lavoro in vista della valutazione di candidati oppure, nel corso del rapporto di lavoro, per l´assegnazione dell´interessato a nuovi incarichi o per selezioni concernenti la progressione di carriera), ma solo di quelli pertinenti rispetto alle finalità di trasparenza perseguite. Prima di pubblicare sul sito istituzionale i curricula, il titolare del trattamento dovrà pertanto operare un'attenta selezione dei dati in essi contenuti. Sarebbe auspicabile che le amministrazioni predisponessero modelli omogenei, impartendo opportune istruzioni agli interessati (che, in concreto, possono essere chiamati a predisporre il proprio curriculum in vista della sua pubblicazione per le menzionate finalità di trasparenza). In tale prospettiva, sono pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative (ad esempio, gli incarichi ricoperti), nonché ulteriori informazioni di carattere professionale (si pensi alle conoscenze linguistiche oppure alle competenze nell'uso delle tecnologie, come pure alla partecipazione a convegni e seminari oppure alla redazione di pubblicazioni da parte dell'interessato). Non devono formare invece oggetto di pubblicazione dati eccedenti, quali ad esempio i recapiti personali oppure il codice fiscale degli interessati, ciò anche al fine di ridurre il rischio di c.d. furti di identità. Deve inoltre essere garantita agli interessati la possibilità di aggiornare periodicamente il proprio curriculum.

L´art. 14 del d.lgs. n 33/2013 dispone la pubblicazione delle "dichiarazioni di cui all'articolo 2, della legge 5 luglio 1982, n. 441, nonché le attestazioni e dichiarazioni di cui agli articoli 3 e 4 della medesima legge, come modificata dal presente decreto, limitatamente al soggetto, al coniuge non separato e ai parenti entro il secondo grado, ove gli stessi vi consentano". Con riferimento all'obbligo di pubblicazione della dichiarazione dei redditi, la predetta disposizione deve essere coordinata con le altre disposizioni dello stesso d.lgs. n. 33/2013 (art. 4, comma 4), con i principi di pertinenza e non eccedenza del RGPD, nonché con le previsioni a tutela dei dati particolari. Pertanto, ai fini dell´adempimento del previsto obbligo di pubblicazione, risulta sufficiente pubblicare copia della dichiarazione dei redditi – dei componenti degli organi di indirizzo politico e, laddove vi acconsentano, del coniuge non separato e dei parenti entro il secondo grado – previo però oscuramento, a cura dell´interessato o del soggetto tenuto alla pubblicazione qualora il primo non vi abbia provveduto, delle informazioni eccedenti e non pertinenti rispetto alla ricostruzione della situazione patrimoniale degli interessati (quali, ad esempio, lo stato civile, il codice fiscale, la sottoscrizione, etc.), nonché di quelle dalle quali si possano desumere indirettamente dati di tipo sensibile, come, fra l´altro, le indicazioni relative a: familiari a carico tra i quali possono essere indicati figli disabili; spese mediche e di assistenza per portatori di handicap o per determinate patologie; erogazioni liberali in denaro a favore dei movimenti e partiti politici; erogazioni liberali in denaro a favore delle organizzazioni non lucrative di utilità sociale, delle iniziative umanitarie, religiose, o laiche, gestite da fondazioni, associazioni, comitati ed enti individuati con decreto del Presidente del Consiglio dei ministri nei paesi non appartenenti all´OCSE; contributi associativi versati dai soci alle società di mutuo soccorso che operano esclusivamente nei settori di cui all´art. 1 della legge 15 aprile 1886, n. 3818, al fine di assicurare ai soci medesimi un sussidio nei casi di malattia, di impotenza al lavoro o di vecchiaia, oppure, in caso di decesso, un aiuto alle loro famiglie; spese sostenute per i servizi di interpretariato dai soggetti riconosciuti sordomuti ai sensi della legge 26 maggio 1970, n. 381; erogazioni liberali in denaro a favore delle istituzioni religiose; scelta per la destinazione dell´otto per mille; scelta per la destinazione del cinque

per mille.

Giova ricordare che non possono essere pubblicati i dati personali del coniuge non separato e dei parenti entro il secondo grado che non abbiano prestato il consenso alla pubblicazione delle attestazioni e delle dichiarazioni di cui all´art. 14, comma 1, lett. f), del d.lgs. n. 33/2013.

La disciplina in materia di trasparenza prevede che informazioni concernenti l'entità di corrispettivi e compensi percepiti da alcune tipologie di soggetti formino oggetto di pubblicazione secondo le modalità previste dal d.lgs. n. 33/2013. Tra questi ultimi sono annoverati, ad esempio, i titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza (cfr. artt. 15 e 41, commi 2 e 3), nonché i dipendenti pubblici cui siano stati conferiti o autorizzati incarichi (art. 18). Pertanto, ai fini dell'adempimento degli obblighi di pubblicazione, risulta proporzionato indicare il compenso complessivo percepito dai singoli soggetti interessati, determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione. Non appare, invece, giustificato riprodurre sul web la versione integrale di documenti contabili, i dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore come pure l'indicazione di altri dati eccedenti riferiti a percettori di somme (quali, ad esempio, i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti). Non risulta inoltre giustificata la pubblicazione di informazioni relative alle dichiarazioni dei redditi dei dipendenti e dei loro familiari, ipotesi questa che la legge impone esclusivamente nei confronti dei componenti degli organi di indirizzo politico (art. 14, del d.lgs. n. 33/2013).

L´art. 23 del d.lgs. n. 33/2013 prevede la pubblicazione obbligatoria di elenchi dei provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti, tra i quali vanno menzionati i provvedimenti finali dei procedimenti relativi alla scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta ai sensi del codice dei contratti pubblici, relativi a lavori, servizi e forniture, di cui al decreto legislativo 18 aprile 2016, n. 50, fermo restando quanto previsto dall'articolo 9-bis e gli accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche, ai sensi degli articoli 11 e 15 della legge 7 agosto 1990, n. 241.

L´art. 26, comma 2, del d.lgs. n. 33/2013 si occupa dell'obbligo di pubblicazione degli atti di concessione "delle sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese, e comunque di vantaggi economici di qualunque genere a persone ed enti pubblici e privati ai sensi del citato articolo 12 della legge n. 241 del 1990, di importo superiore a mille euro". Il comma 3 del medesimo articolo aggiunge che tale pubblicazione "costituisce condizione legale di efficacia dei provvedimenti che dispongano concessioni e attribuzioni di importo complessivo superiore a mille euro nel corso dell'anno solare al medesimo beneficiario". In merito alle predette pubblicazioni è prevista l´indicazione delle seguenti informazioni: a) il nome dell´impresa o dell´ente e i rispettivi dati fiscali o il nome di altro soggetto beneficiario; b) l´importo del vantaggio economico corrisposto; c) la norma o il titolo a base dell´attribuzione; d) l´ufficio e il funzionario o dirigente responsabile del relativo procedimento amministrativo; e) la modalità seguita per l´individuazione del beneficiario; f) il link al progetto selezionato e al curriculum del soggetto incaricato (art. 27, comma 1). In tale quadro, lo stesso d.lgs. n. 33/2013 individua una serie di limiti all'obbligo di pubblicazione di atti di concessione di benefici economici comunque denominati. Non possono, infatti, essere pubblicati i dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici, nonché gli elenchi dei relativi destinatari: a) di importo complessivo inferiore a mille euro nel corso dell´anno solare a favore del medesimo beneficiario; b) di importo superiore a mille euro nel corso dell´anno solare a favore del medesimo beneficiario "qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute" (art. 26, comma 4, d.lgs. n. 33/2013; nonché artt. 22, comma 8, e 68, comma 3, del Codice); c) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario "qualora da tali dati sia possibile ricavare informazioni relative […] alla situazione di disagio economico-sociale degli interessati" (art. 26, comma 4, d.lgs. n. 33/2013).

Si ribadisce, con specifico riferimento alle informazioni idonee a rivelare lo stato di

salute, che è vietata la diffusione di qualsiasi dato o informazione da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. Si pensi, ad esempio, all'indicazione della disposizione sulla base della quale ha avuto luogo l´erogazione del beneficio economico se da essa è possibile ricavare informazioni sullo stato di salute di una persona o dei titoli dell´erogazione dei benefici (es. attribuzione di borse di studio a "soggetto portatore di handicap", o riconoscimento di buono sociale a favore di "anziano non autosufficiente" o con l´indicazione, insieme al dato anagrafico, delle specifiche patologie sofferte dal beneficiario); delle modalità e dei criteri di attribuzione del beneficio economico (es. punteggi attribuiti con l´indicazione degli "indici di autosufficienza nelle attività della vita quotidiana" ; della destinazione dei contributi erogati (es. contributo per "ricovero in struttura sanitaria" o per "assistenza sanitaria").

È, inoltre, vietato riportare dati o informazioni da cui si può desumere la condizione di indigenza o di disagio sociale in cui versano gli interessati (art. 26, comma 4, del d.lgs. n. 33/2013).

Si tratta di un divieto funzionale alla tutela della dignità, dei diritti e delle libertà fondamentali dell'interessato, al fine di evitare che soggetti che si trovano in condizioni disagiate – economiche o sociali – soffrano l'imbarazzo della diffusione di tali informazioni, o possano essere sottoposti a conseguenze indesiderate, a causa della conoscenza da parte di terzi della particolare situazione personale. Si pensi, fra l'altro alle fasce deboli della popolazione (persone inserite in programmi di recupero e di reinserimento sociale, anziani, minori di età, etc.). Alla luce delle considerazioni sopra espresse, spetta agli enti destinatari degli obblighi di pubblicazione online contenuti nel d.lgs. n. 33/2013, in quanto titolari del trattamento, valutare, caso per caso, quando le informazioni contenute nei provvedimenti rivelino l'esistenza di una situazione di disagio economico o sociale in cui versa il destinatario del beneficio e non procedere, di conseguenza, alla pubblicazione dei dati identificativi del beneficiario o delle altre informazioni che possano consentirne l'identificazione. Tale decisione rimane comunque sindacabile da parte del Garante che assicura il rispetto dei già menzionati principi in materia di protezione dei dati personali. In ogni modo, si evidenzia che i soggetti destinatari degli obblighi di pubblicazione contenuti nel d.lgs. n. 33/2013 sono tenuti, anche in tale ambito, al rispetto dei principi di minimizzazione, pertinenza e non eccedenza, nonché delle disposizioni a tutela dei dati particolari.

"Non risulta, pertanto, giustificato diffondere, fra l´altro, dati quali, ad esempio, l´indirizzo di abitazione o la residenza, il codice fiscale di persone fisiche, le coordinate bancarie dove sono accreditati i contributi o i benefici economici (codici IBAN), la ripartizione degli assegnatari secondo le fasce dell´Indicatore della situazione economica equivalente-Isee, l´indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative, etc. Si evidenzia, inoltre, che il riutilizzo dei dati personali pubblicati ai sensi dei predetti artt. 26 e 27, non è libero, ma subordinato – come stabilito dallo stesso art. 7 del d.lgs. n. 33/2013 – alle specifiche disposizioni di cui alla direttiva comunitaria 2003/98/CE e al d.lgs. n. 36 del 24 gennaio 2006 di recepimento della stessa, che non pregiudicano in alcun modo il livello di tutela delle persone con riguardo al trattamento dei dati personali"[45].

L'assolvimento degli obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici descritti nel paragrafo precedente deve essere coordinato con le disposizioni che regolano la predisposizione dell´albo dei beneficiari di provvidenze di natura economica (d.P.R. 7 aprile 2000, n. 118).

Per tale motivo, alla luce di un'interpretazione sistematica del quadro normativo emergente dalla recente novella in tema di trasparenza e al fine di non duplicare in capo alle pubbliche amministrazioni gli oneri di pubblicazione, deve ritenersi che l'adempimento delle prescrizioni contenute negli artt. 26 e 27 del d.lgs. n. 33/2013, con le relative modalità ed eccezioni descritte nel

[45] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, 15 maggio 2014, doc. web 3134436.

paragrafo precedente, assorbe gli obblighi previsti dagli artt. 1 e 2 del d.P.R. n. 118.

Gran parte delle indicazioni fornite dal Garante per la protezione dei dati personali contenute nelle linee guida del 15 maggio 2014 sono state riprese dall'Autorità Nazionale Anticorruzione con la delibera n. 1310 del 28 dicembre 2016: *Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016*.

Le linee guida del Garante del 15 maggio 2014, come già rilevato, hanno lo scopo di definire un quadro unitario di misure e accorgimenti diretti a individuare opportune cautele che i soggetti pubblici, e gli altri soggetti parimenti destinatari delle norme vigenti, sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa. Pertanto, le predette linee guida sostituiscono le precedenti "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" del 2 marzo 2011 (doc. web n. 1793203).

Le linee guida del 15 maggio 2014 vanno lette in relazione al profilo del diverso regime giuridico applicabile, le disposizioni che regolano gli obblighi di pubblicità dell'azione amministrativa per finalità di trasparenza vanno distinte da quelle che regolano forme di pubblicità per finalità diverse (es.: pubblicità legale). Come più volte rilevato, gli obblighi di pubblicazione online di dati per finalità di trasparenza sono quelli indicati nel d.lgs. n. 33/2013 e agli obblighi introdotti dalla predetta normativa si applicano le indicazioni contenute nella parte prima delle suddette linee guida.

Accanto a questi obblighi di pubblicazione permangono altri obblighi di pubblicità online di dati, informazioni e documenti della pubblica amministrazione, contenuti in specifiche disposizioni di settore diverse da quelle approvate in materia di trasparenza, come, fra l´altro, quelli volti a far conoscere l´azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli atti a garantire la pubblicità legale degli atti amministrativi (es.: pubblicità integrativa dell´efficacia, dichiarativa, notizia). Si pensi, a titolo meramente esemplificativo, alle pubblicazioni ufficiali dello Stato, alle pubblicazioni di deliberazioni, ordinanze e determinazioni sull´albo pretorio online degli enti locali (oppure su analoghi albi di altri enti, come ad esempio le Asp), alle pubblicazioni matrimoniali, alla pubblicazione degli atti concernenti il cambiamento del nome, alla pubblicazione della comunicazione di avviso deposito delle cartelle esattoriali a persone irreperibili, ai casi di pubblicazione dei ruoli annuali tributari dei consorzi di bonifica, alla pubblicazione dell´elenco dei giudici popolari di corte d´assise, etc. A tali obblighi si riferiscono le indicazioni contenute nella parte seconda delle linee guida del 15 maggio 2014.

Il d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, ha operato una significativa estensione dei confini della trasparenza intesa oggi come «accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche». Il legislatore ha attribuito un ruolo di primo piano alla trasparenza affermando, tra l'altro, che essa concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Essa è anche da considerare come condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integrando il diritto ad una buona amministrazione e concorrendo alla realizzazione di una amministrazione aperta, al servizio del cittadino. Oggi, dunque, la trasparenza è anche regola per l'organizzazione, per l'attività amministrativa e per la realizzazione di una moderna democrazia. In tal senso si è espresso anche il Consiglio di Stato laddove ha ritenuto che "la trasparenza viene a configurarsi, ad un tempo, come un mezzo per porre in essere una azione amministrativa più efficace e conforme ai canoni costituzionali e come un obiettivo a cui tendere, direttamente legato al valore democratico della funzione amministrativa" (Cons. Stato., Sez. consultiva per gli atti normativi, 24 febbraio 2016, n. 515, parere reso sullo schema di decreto n.

97/2016). Le disposizioni in materia di trasparenza amministrativa, inoltre, integrano l'individuazione del livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche a fini di trasparenza, prevenzione, contrasto della corruzione e della cattiva amministrazione, a norma dell'art. 117, co. 2, lett. m), della Costituzione (art. 1, co. 3, d.lgs. 33/2013). La trasparenza assume, così, rilievo non solo come presupposto per realizzare una buona amministrazione ma anche come misura per prevenire la corruzione, promuovere l'integrità e la cultura della legalità in ogni ambito dell'attività pubblica, come già l'art. 1, co. 36 della legge 190/2012 aveva sancito. Dal richiamato comma si evince, infatti, che i contenuti del d.lgs. 33/2013 «integrano l'individuazione del livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche a fini di trasparenza, prevenzione, contrasto della corruzione e della cattiva amministrazione». La stessa Corte Costituzionale (sent. 20/2019) ha considerato che con la legge 190/2012 «la trasparenza amministrativa viene elevata anche al rango di principio-argine alla diffusione di fenomeni di corruzione» e che le modifiche al d.lgs. 33/2013, introdotte dal d.lgs. n. 97/2016, hanno esteso ulteriormente gli scopi perseguiti attraverso il principio di trasparenza, aggiungendovi la finalità di «tutelare i diritti dei cittadini» e "promuovere la partecipazione degli interessati all'attività amministrativa". La Corte ha riconosciuto, inoltre, che i principi di pubblicità e trasparenza trovano riferimento nella Costituzione italiana in quanto corollario del principio democratico (art. 1 Cost.) e del buon funzionamento dell'amministrazione (art. 97 Cost.). L'ampliamento dei confini della trasparenza registrato nel nostro ordinamento, appena illustrato, è stato realizzato con successive modifiche normative che sono state accompagnate da atti di regolazione dell'Autorità finalizzati a fornire indicazioni ai soggetti tenuti ad osservare la disciplina affinché l'attuazione degli obblighi di pubblicazione non fosse realizzata in una logica di mero adempimento quanto, invece, di effettività e piena conoscibilità dell'azione amministrativa.

Come rilevato da attenta dottrina[46], una delle novità importanti è contenuta nell'art. 2, il quale non si limita solo a richiamare lo scopo della trasparenza intesa come accessibilità totale: non si tratta solo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche, ma anche di tutelare i diritti fondamentali. La trasparenza è, infatti, condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto a una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino.

Lo scopo della norma è quello di garantire la conoscibilità dei documenti e dei dati relativi prodotti dalle amministrazioni, nonché la libertà di accesso a dati e documenti (oggetto di pubblicazione obbligatoria) in possesso della pubblica amministrazione attraverso l'accesso civico "semplice", ma anche attraverso l'accesso civico "generalizzato" relativamente ai dati e ai documenti detenuti dalle amministrazioni ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria (aspetto questo che sarà ripreso e approfondito nel prosieguo).

Tutti i documenti, le informazioni e i dati oggetto di accesso civico, ivi compresi quelli oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'art. 7 del d.lgs n. 33/2013.

Il decreto introduce, al riguardo, la nozione di accesso civico, per distinguerla da quella di accesso ai sensi degli articoli 22 ss. della legge n. 241/1990 sul procedimento amministrativo (articolo 5). Con essa, s'intende, il diritto di chiunque di richiedere alle pubbliche amministrazioni i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria, nei casi in cui questa sia stata omessa. A differenza del diritto di accesso agli atti di cui alla legge 241/1990, la richiesta di accesso civico non è sottoposta ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente, siamo, infatti, in presenza di un diritto a titolarità diffusa. Non è soggetto, inoltre, a motivazione.

"La giuridicizzazione di un tale ambito di trasparenza si traduce nella pubblicità di una serie di informazioni, che conferma la distanza, sul piano del diritto positivo, tra accesso e trasparenza, in quanto il primo,

[46] D. Urania Galletta, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *Fedaralismi.it*, 2016.

come posizione qualificata da un criterio di collegamento specifico tra richiedente l'accesso e il dato che si vuole conoscere, non ha evidentemente spazio per operare laddove quel dato sia pubblico perché accessibile all'intera collettività. In tale ottica la trasparenza, pur sempre riferibile al duplice versante organizzativo e "attivo" dell'amministrazione e quindi al procedimento amministrativo, acquista una sua ragion d'essere anche, e forse soprattutto, al di fuori dello schema e del momento procedimentale in senso stretto"[47].

Con l'accesso civico il legislatore introduce un meccanismo rimediale di assoluta novità, riconoscendo in capo a chiunque un vero e proprio diritto di accesso civico a quelle informazioni e a quei dati (siano o meno contenuti in atti giuridici in senso stretto) per i quali risulti non adempiuto l'obbligo di pubblicità: un diritto di accesso, quindi, svincolato dai requisiti di legittimazione dell'accesso previsto dalla legge n. 241 del 1990, azionabile senza formalità, senza necessità di motivare l'istanza, senza dover dimostrare l'utilità dell'atto che si intende conoscere rispetto alle esigenze difensive del richiedente, ma fondato sul solo presupposto dell'inadempimento in cui l'amministrazione è incorsa rispetto agli obblighi di pubblicità.

Gli obblighi di pubblicazione, previsti dal decreto, integrano una "situazione che fronteggia (...) un diritto soggettivo a conoscere, che spetta a "chiunque", ossia ai cittadini in quanto tali (senza necessità di dimostrare l'interesse differenziato che giustifichi tale pretesa) (art. 3). Agli obblighi di pubblicazione corrisponde dunque non un *need to know* (una conoscenza utile al soddisfacimento di un interesse, di un bisogno particolare), ma un vero *right to know*. Un diritto conseguentemente assistito da un meccanismo di implementazione (in caso di inadempimento dell'obbligo di pubblicazione) attivabile da chiunque, quasi nella forma dell'azione popolare"[48].

Il legislatore nel 2016 al fine di dare forza e vigore al principio del controllo diffuso della generalità dei cittadini, inteso come controllo democratico e carattere essenziale della trasparenza pubblica delle istituzioni pubbliche, ha introdotto nel nostro ordinamento giuridico l'istituto dell'accesso civico "generalizzato": "Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis" (art. 5, c. 2, del d.lgs. n. 33/2013).

La Corte Costituzionale, chiamata ad esprimersi sul tema del bilanciamento tra diritto alla riservatezza dei dati personali, inteso come diritto a controllare la circolazione delle informazioni riferite alla propria persona, e quello dei cittadini al libero accesso ai dati ed alle informazioni detenuti dalle pubbliche amministrazioni, ha riconosciuto che entrambi i diritti sono «contemporaneamente tutelati sia dalla Costituzione che dal diritto europeo, primario e derivato» (Corte Cost., 23 gennaio 2019, n. 20).

Ritiene la Corte che, se da una parte il diritto alla riservatezza dei dati personali, quale manifestazione del diritto fondamentale all'intangibilità della sfera privata, attiene alla tutela della vita degli individui nei suoi molteplici aspetti e trova sia riferimenti nella Costituzione italiana (artt. 2, 14, 15 Cost.), sia specifica protezione nelle varie norme europee e convenzionali, dall'altra parte, con eguale rilievo, si incontrano i principi di pubblicità e trasparenza, riferiti non solo, quale corollario del principio democratico (art. 1 Cost.) a tutti gli aspetti rilevanti della vita pubblica e istituzionale, ma anche, ai sensi dell'art. 97 Cost., al buon funzionamento dell'amministrazione e ai dati che essa possiede e controlla. Principi che, nella legislazione interna, si manifestano nella loro declinazione soggettiva, nella forma di un diritto dei cittadini ad accedere ai dati in possesso della pubblica amministrazione, come stabilito dall'art. 1, co. 1, del d.lgs. n. 33/2013.

Il bilanciamento tra i due diritti è, quindi, necessario, come lo stesso Considerando n. 4

[47] F. Patroni Griffi, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *Federalismi.it*, 2013.

[48] B. Ponti, *Il codice della trasparenza amministrativa: non solo riordino, ma ridefinizione complessiva del regime della trasparenza amministrativa on-line*, in *www.neldiritto.it*.

del Regolamento (UE) 2016/679 indica, prevedendo che «Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità».

In particolare, nella richiamata sentenza, la Corte precisa che il bilanciamento della trasparenza e della privacy va compiuto avvalendosi del test di proporzionalità che "richiede di valutare se la norma oggetto di scrutinio, con la misura e le modalità di applicazione stabilite, sia necessaria e idonea al conseguimento di obiettivi legittimamente perseguiti, in quanto, tra più misure appropriate, prescriva quella meno restrittiva dei diritti a confronto e stabilisca oneri non sproporzionati rispetto al perseguimento di detti obiettivi". L'art. 3 Cost., integrato dai principi di derivazione europea, sancisce l'obbligo, per la legislazione nazionale, di rispettare i criteri di necessità, proporzionalità, finalità, pertinenza e non eccedenza nel trattamento dei dati personali, pur al cospetto dell'esigenza di garantire, fino al punto tollerabile, la pubblicità dei dati in possesso della pubblica amministrazione.

Pertanto, al principio di trasparenza, nonostante non trovi espressa previsione nella Costituzione, si riconosce rilevanza costituzionale, in quanto fondamento di diritti, libertà e principi costituzionalmente garantiti (artt. 1 e 97 Cost.).

Il quadro delle regole in materia di protezione dei dati personali si è consolidato con l'entrata in vigore, il 25 maggio 2018, del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito RGPD) e, il 19 settembre 2018, del decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali – decreto legislativo 30 giugno 2003, n. 196 - alle disposizioni del Regolamento (UE) 2016/679.

Occorre evidenziare che l'art. 2-ter del d.lgs. n. 196 del 2003, introdotto dal d.lgs. 101/2018, in continuità con il previgente articolo 19 del Codice, dispone al comma 1 che la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ai sensi dell'art. 6, paragrafo 3, lett. b) del Regolamento (UE) 2016/679, "è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento». Inoltre, il comma 3 del medesimo articolo stabilisce che «La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1».

Il regime normativo per il trattamento di dati personali da parte dei soggetti pubblici è, quindi, rimasto sostanzialmente inalterato, essendo confermato il principio che esso è consentito unicamente se ammesso da una norma di legge o, nei casi previsti dalla legge, di regolamento.

La nuova tipologia di accesso (d'ora in poi "accesso generalizzato"), delineata nel novellato art. 5, comma 2 del d.lgs. n. 33/2013, ai sensi del quale "chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, secondo quanto previsto dall'art. 5-bis", si traduce, in estrema sintesi, in un diritto di accesso non condizionato dalla titolarità di situazioni giuridicamente rilevanti ed avente ad oggetto tutti i dati e i documenti e informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli per i quali è stabilito un obbligo di pubblicazione.

La ratio della riforma risiede nella dichiarata finalità di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico (art. 5, comma 2, d.lgs. n. 33/2013).

A questa impostazione, come mette in luce l'ANAC nella determinazione n. 1309 del 28 dicembre 2016 redatta d'intesa con il Garante per la protezione dei dati personali, consegue, nel novellato decreto 33/2013, il rovesciamento della precedente prospettiva che comportava l'attivazione del diritto di accesso civico solo strumentalmente all'adempimento degli obblighi di pubblicazione; ora è proprio la libertà di accedere ai dati e ai documenti, cui corrisponde una diversa versione dell'accesso civico, a divenire centrale nel nuovo sistema, in analogia agli ordinamenti aventi il *Freedom of Information Act* (FOIA), ove il diritto

all'informazione è generalizzato e la regola generale è la trasparenza mentre la riservatezza e il segreto eccezioni.

In coerenza con il quadro normativo, il diritto di accesso civico generalizzato si configura come diritto a titolarità diffusa, potendo essere attivato "da chiunque" e non essendo sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente. A ciò si aggiunge un ulteriore elemento, ossia che l'istanza "non richiede motivazione". In altri termini, tale nuova tipologia di accesso civico risponde all'interesse dell'ordinamento di assicurare ai cittadini (a "chiunque"), indipendentemente dalla titolarità di situazioni giuridiche soggettive, un accesso a dati, documenti e informazioni detenute da pubbliche amministrazioni e dai soggetti indicati nell'art. art. 2-bis del d.lgs. 33/2013 come modificato dal d.lgs. n. 97/2016.

L'accesso generalizzato deve essere anche tenuto distinto dalla disciplina dell'accesso ai documenti amministrativi di cui agli articoli 22 e seguenti della legge 7 agosto 1990, n. 241.

La finalità dell'accesso documentale ex legge 241/90 è, in effetti, ben differente da quella sottesa all'accesso generalizzato ed è quella di porre i soggetti interessati in grado di esercitare al meglio le facoltà - partecipative e/o oppositive e difensive – che l'ordinamento attribuisce loro a tutela delle posizioni giuridiche qualificate di cui sono titolari. Più precisamente, dal punto di vista soggettivo, ai fini dell'istanza di accesso ex legge 241 il richiedente deve dimostrare di essere titolare di un «interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso». Mentre la legge 241/90 esclude, inoltre, perentoriamente l'utilizzo del diritto di accesso ivi disciplinato al fine di sottoporre l'amministrazione a un controllo generalizzato.

Dunque, l'accesso agli atti di cui alla legge 241/90 continua certamente a sussistere, ma parallelamente all'accesso civico (generalizzato e non), operando sulla base di norme e presupposti diversi. Tenere ben distinte le due fattispecie è essenziale per calibrare i diversi interessi in gioco allorché si renda necessario un bilanciamento caso per caso tra tali interessi. Tale bilanciamento è, infatti, ben diverso nel caso dell'accesso 241 dove la tutela può consentire un accesso più in profondità a dati pertinenti e nel caso dell'accesso generalizzato, dove le esigenze di controllo diffuso del cittadino devono consentire un accesso meno in profondità (se del caso, in relazione all'operatività dei limiti) ma più esteso, avendo presente che l'accesso in questo caso comporta, di fatto, una larga conoscibilità (e diffusione) di dati, documenti e informazioni.

Data l'innovatività della disciplina dell'accesso generalizzato, che si aggiunge alle altre tipologie di accesso, sembra opportuno suggerire ai soggetti tenuti all'applicazione del decreto trasparenza l'adozione, anche nella forma di un regolamento interno sull'accesso, di una disciplina che fornisca un quadro organico e coordinato dei profili applicativi relativi alle tre tipologie di accesso, con il fine di dare attuazione al nuovo principio di trasparenza introdotto dal legislatore e di evitare comportamenti disomogenei tra uffici della stessa amministrazione.

In particolare, tale disciplina potrebbe prevedere: 1. una sezione dedicata alla disciplina dell'accesso documentale; 2. una seconda sezione dedicata alla disciplina dell'accesso civico ("semplice") connesso agli obblighi di pubblicazione di cui al d.lgs. n. 33; 3. una terza sezione dedicata alla disciplina dell'accesso generalizzato. Tale sezione dovrebbe disciplinare gli aspetti procedimentali interni per la gestione delle richieste di accesso generalizzato. Si tratterebbe, quindi, di: a) provvedere a individuare gli uffici competenti a decidere sulle richieste di accesso generalizzato; b) provvedere a disciplinare la procedura per la valutazione caso per caso delle richieste di accesso.

La regola della generale accessibilità è temperata dalla previsione di eccezioni poste a tutela di interessi pubblici e privati che possono subire un pregiudizio dalla diffusione generalizzata di talune informazioni. Dalla lettura dell'art. 5 bis, co. 1, 2 e 3 del d.lgs. n. 33/2013 si possono distinguere due tipi di eccezioni, assolute o relative.

Al ricorrere di queste eccezioni, le amministrazioni, rispettivamente, devono o possono rifiutare l'accesso generalizzato. La chiara identificazione di tali eccezioni rappresenta un elemento decisivo per consentire la corretta applicazione del diritto di accesso generalizzato.

Tra le eccezioni assolute all'accesso generalizzato, Salvo che non sia possibile un accesso parziale, con oscuramento dei dati, alcuni divieti di divulgazione sono previsti dalla normativa vigente in materia di tutela della riservatezza con riferimento a: dati idonei a rivelare lo stato di salute, ossia a qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici (art. 22, comma 8, del Codice; art. 7-bis, comma 6, d.lgs. n. 33/2013); dati idonei a rivelare la vita sessuale (art. 7-bis, comma 6, d.lgs. n. 33/2013); dati identificativi di persone fisiche beneficiarie di aiuti economici da cui è possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati (limite alla pubblicazione previsto dall'art. 26, comma 4, d.lgs. n. 33/2013).

Resta, in ogni caso, ferma la possibilità che i dati personali per i quali sia stato negato l'accesso generalizzato possano essere resi ostensibili al soggetto che abbia comunque motivato nell'istanza l'esistenza di «un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso», trasformando di fatto, con riferimento alla conoscenza dei dati personali, l'istanza di accesso generalizzato in un'istanza di accesso ai sensi della legge 241/1990.

Accanto alle eccezioni assolute, la normativa ha individuato limiti relativi a tutela di interessi privati. Il d.lgs. n. 33/2013 ha previsto, all'art. 5-bis, comma 2, che l'accesso generalizzato è rifiutato se il diniego è necessario per evitare il pregiudizio concreto alla tutela degli interessi privati specificamente indicati dalla norma e cioè:

a) protezione dei dati personali

b) libertà e segretezza della corrispondenza

c) interessi economici e commerciali di una persona fisica o giuridica, ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali.

L'art. 5-bis, comma 2, lett. a), del d.lgs. n. 33/2013 prevede che l'accesso generalizzato deve essere rifiutato laddove possa recare un pregiudizio concreto «alla protezione dei dati personali, in conformità con la disciplina legislativa in materia». Le informazioni riferite a persone giuridiche, enti e associazioni non rientrano nella nozione di dato personale.

Con riferimento alle istanze di accesso generalizzato aventi a oggetto dati e documenti relativi a (o contenenti) dati personali, l'ente destinatario dell'istanza deve valutare, nel fornire riscontro motivato a richieste di accesso generalizzato, se la conoscenza da parte di chiunque del dato personale richiesto arreca (o possa arrecare) un pregiudizio concreto alla protezione dei dati personali, in conformità alla disciplina legislativa in materia. La ritenuta sussistenza di tale pregiudizio comporta il rigetto dell'istanza, a meno che non si consideri di poterla accogliere, oscurando i dati personali eventualmente presenti e le altre informazioni che possono consentire l'identificazione, anche indiretta, del soggetto interessato devono essere tenute in considerazione le motivazioni addotte dal soggetto controinteressato, che deve essere obbligatoriamente interpellato dall'ente destinatario della richiesta di accesso generalizzato, ai sensi dell'art. 5, comma 5, del d.lgs. n. 33/2013. Tali motivazioni costituiscono un indice della sussistenza di un pregiudizio concreto, la cui valutazione però spetta all'ente e va condotta anche in caso di silenzio del controinteressato.

Il soggetto destinatario dell'istanza, nel dare riscontro alla richiesta di accesso generalizzato, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei dati personali in esso presenti, laddove l'esigenza informativa, alla base dell'accesso generalizzato, possa essere raggiunta senza implicare il trattamento dei dati personali. In tal modo, tra l'altro, si soddisfa anche la finalità di rendere più celere il procedimento relativo alla richiesta di accesso generalizzato, potendo accogliere l'istanza senza dover attivare l'onerosa procedura di coinvolgimento del soggetto "controinteressato" (art. 5, comma 5, del d.lgs. n. 33/2013).

Al riguardo, deve essere ancora evidenziato che l'accesso generalizzato è servente rispetto alla conoscenza di dati e documenti detenuti dalla pubblica amministrazione "Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di

promuovere la partecipazione al dibattito pubblico" (art. 5, comma 2, del d.lgs. n. 33/2013). Di conseguenza, quando l'oggetto della richiesta di accesso riguarda documenti contenenti informazioni relative a persone fisiche (e in quanto tali dati personali) non necessarie al raggiungimento del predetto scopo, oppure informazioni personali di dettaglio che risultino comunque sproporzionate, eccedenti e non pertinenti, l'ente destinatario della richiesta dovrebbe accordare l'accesso parziale ai documenti, oscurando i dati personali ivi presenti.

Ai fini della valutazione del pregiudizio concreto, vanno prese in considerazione le conseguenze – anche legate alla sfera morale, relazionale e sociale – che potrebbero derivare all'interessato (o ad altre persone alle quali esso è legato da un vincolo affettivo) dalla conoscibilità, da parte di chiunque, del dato o del documento richiesto, tenuto conto delle implicazioni derivanti dalla previsione di cui all'art. 3, comma 1, del d.lgs. n. 33/2013, in base alla quale i dati e i documenti forniti al richiedente tramite l'accesso generalizzato sono considerati come pubblici, sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 7 del d.lgs. n. 33/2013).

Tali conseguenze potrebbero riguardare, ad esempio, future azioni da parte di terzi nei confronti dell'interessato, o situazioni che potrebbero determinare l'estromissione o la discriminazione dello stesso individuo, oppure altri svantaggi personali e/o sociali. In questo quadro, può essere valutata, ad esempio, l'eventualità che l'interessato possa essere esposto a minacce, intimidazioni, ritorsioni o turbative al regolare svolgimento delle funzioni pubbliche o delle attività di pubblico interesse esercitate, che potrebbero derivare, a seconda delle particolari circostanze del caso, dalla conoscibilità di determinati dati. Analogamente, vanno tenuti in debito conto i casi in cui la conoscibilità di determinati dati personali da parte di chiunque possa favorire il verificarsi furti d'identità o di creazione di identità fittizie.

Per verificare l'impatto sfavorevole che potrebbe derivare all'interessato dalla conoscibilità da parte di chiunque delle informazioni richieste, l'ente destinatario della richiesta di accesso generalizzato deve far riferimento a diversi parametri, tra i quali, anche la natura dei dati personali oggetto della richiesta di accesso o contenuti nei documenti ai quali di chiede di accedere, nonché il ruolo ricoperto nella vita pubblica, la funzione pubblica esercitata o l'attività di pubblico interesse svolta dalla persona cui si riferiscono i predetti dati.

Riguardo al primo profilo, la presenza di dati sensibili e/o giudiziari può rappresentare un indice della sussistenza del predetto pregiudizio, laddove la conoscenza da parte di chiunque che deriverebbe dall'ostensione di tali informazioni – anche in contesti diversi (familiari e/o sociali) – possa essere fonte di discriminazione o foriera di rischi specifici per l'interessato. In linea di principio, quindi, andrebbe rifiutato l'accesso generalizzato a tali informazioni, potendo invece valutare diversamente, caso per caso, situazioni particolari quali, ad esempio, quelle in cui le predette informazioni siano state deliberatamente rese note dagli interessati, anche attraverso loro comportamenti in pubblico.

Analoghe considerazioni sull'esistenza del pregiudizio concreto possono essere fatte per quelle categorie di dati personali che, pur non rientrando nella definizione di dati sensibili e giudiziari, richiedono una specifica protezione quando dal loro utilizzo, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, possano derivare rischi specifici per i diritti e le libertà fondamentali degli interessati (si pensi, ad esempio, ai dati genetici, biometrici, di profilazione, sulla localizzazione o sulla solvibilità economica).

Tra gli altri fattori da tenere in considerazione ai fini della valutazione della sussistenza del pregiudizio in esame, merita rilievo anche la circostanza che la richiesta di accesso generalizzato riguardi dati o documenti contenenti dati personali di soggetti minori, la cui conoscenza può ostacolare il libero sviluppo della loro personalità, in considerazione della particolare tutela dovuta alle fasce deboli.

Riguardo al secondo profilo, va considerato altresì che la sussistenza di un pregiudizio concreto alla protezione dei dati personali può verificarsi con più probabilità per talune particolari informazioni – come ad esempio situazioni personali, familiari, professionali, patrimoniali – di persone fisiche destinatarie dell'attività amministrativa o intervenute a vario titolo nella stessa e che, quindi, non ricoprono necessariamente un ruolo nella vita

pubblica o non esercitano funzioni pubbliche o attività di pubblico interesse.

8. *Smart working e protezione dei dati personali nella Pubblica Amministrazione*

«Michel de Montaigne ci ricordava che "la vie est un mouvement inégal, irrégulier et multiforme" (*Essais*, Livre III, Chap. III, De trois commerces). Questo movimento è oggi sempre più influenzato dall'incessante innovazione scientifica e tecnologica. I ritmi della vita conoscono accelerazioni e mutamenti profondi», così Stefano Rodotà apriva uno dei suoi tanti studi dedicati al rapporto tra nuove tecnologie e diritti della persona[49]. Tutto ciò lo abbiamo constatato, ormai da più di due anni, a seguito dell'improvvisa e inattesa accelerazione impressa dalla pandemia da Sars-CoV-2 alla transizione digitale, che ci ha imposto di ripensare, con altrettanta rapidità, il nostro modo di concepire questa nuova dimensione della vita. Come rilevato da Antonello Soro, "la devoluzione alla dimensione immateriale di quasi tutte le nostre attività è un processo neutro, ma comporta, se non assistito da adeguate garanzie, l'esposizione a inattese vulnerabilità in termini non solo di sicurezza informatica, ma anche di soggezione a intrusioni e controlli sempre più penetranti e pericolosi, poiché meno percettibili rispetto a quelli "tradizionali"[50].

Pensiamo, ad esempio, al contesto lavorativo e, al fenomeno, in particolare, dello *smart working*, generalmente necessitato e improvvisato, che ha catapultato migliaia di lavoratori in una dimensione delle cui implicazioni, il più delle volte, non si ha la piena consapevolezza e di cui occorre impedire un uso improprio. L'inarrestabile processo di digitalizzazione e l'emergere di nuovi processi economici sono questioni ampiamente trattati nella letteratura sociologica ed economico-aziendale, nonché entrati da tempo nell'agenda delle istituzioni europee. Le analisi si concentrano, in particolare, "sui fattori innovativi e sulle caratteristiche degli scenari in divenire, con l'obiettivo di discernere ciò che costituisce un'autentica rottura rispetto al passato e ciò che rappresenta invece un'accelerazione di tendenze già presenti nei processi di ristrutturazione produttiva delle imprese e nelle trasformazioni del lavoro"[51]. Lo *smart working*, potendo favorire una nuova articolazione dei processi produttivi in grado di accrescere efficienza e flessibilità, potrebbe costituire una forma diffusa, alternativa, di organizzazione del lavoro. Per questo motivo andranno affrontati con serietà e lungimiranza tutti i problemi emersi in questi mesi, a seguito della pandemia: dalle dotazioni strumentali alla garanzia di connettività, alla sicurezza delle piattaforme, all'effettività del diritto alla disconnessione, senza il quale si rischia di rendere vana la necessaria distinzione tra sfera privata e attività lavorativa.

Lo *smart working* è una rivoluzione culturale, organizzativa e di processo. Una rivoluzione poiché scardina alla base consuetudini e approcci tradizionali e consolidati nel mondo del lavoro subordinato, fondandosi su una cultura orientata ai risultati e su una valutazione legata alle reali performance. Secondo la definizione data il Ministero del Lavoro e delle Politiche Sociali, lo *smart working* è una modalità di esecuzione del rapporto subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi, cicli e obiettivi, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività".

La legge 22 maggio 2017 n. 81 (art. 18-24) ha fornito allo *smart working* una cornice normativa e ha posto le basi legali per la sua applicazione anche nel settore pubblico. La

[49] S. Rodotà, *Persona, libertà, tecnologia. Note per una discussione*, in www.dirittoequestionipubbliche.org/page/2005_n5/mono_S_Rodota.pdf.

[50] A. Soro, *Relazione 2019* del Garante per la protezione dei dati personali (www.garanteprivacy.it).

[51] P. Tullini, *Uso delle tecnologie al lavoro. Il controllo a distanza e le garanzie del lavoratore*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, Giappichelli, 2017, 4; A. Bellavista, *Sorveglianza sui lavoratori, protezione dei dati personali e azione collettiva nell'economia digitale*, in C. Alessi, M. Barbera, L. Guaglianone (a cura di), *Impresa, lavoro e non lavoro nell'economia digitale*, Bari, Cacucci Editore, 2019, 151 ss.; P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, Giappichelli, 2017; A. Sartori, *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Torino, Giappichelli, 2020; C. Colapietro, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Giornale di diritto del lavoro e di relazioni industriali*, 2017, 439 ss.; G. Ziccardi, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *Labour & Law Issues*, 2016, 1 ss.

legge all'art. 18 definisce il lavoro agile (*smart working*) come "modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva". Obiettivo dichiarato è promuovere il lavoro agile per "incrementare la competitività e agevolare la conciliazione dei tempi di vita e di lavoro". Il comma 3, sempre del richiamato art. 18, precisa che le disposizioni normative si applicano anche ai "rapporti di lavoro alle dipendenze delle amministrazioni pubbliche". Con la successiva direttiva n. 3 del 2017 del Ministro per la Pubblica Amministrazione ha preso avvio "ufficialmente" la stagione del "lavoro agile" o *smart working* nelle pubbliche amministrazioni. Detta direttiva contiene gli indirizzi per l'attuazione dei commi 1 e 2 dell'art. 14 della legge 7 agosto 2015, n. 124, che delegava il Governo alla riorganizzazione delle amministrazioni pubbliche, prevedendo l'introduzione di nuove e più agili misure di conciliazione dei tempi di vita e di lavoro dei propri dipendenti, e individua le linee guida per la nuova organizzazione del lavoro, finalizzate a promuovere la conciliazione dei tempi di vita e di lavoro dei dipendenti. Le finalità dichiarate sono quelle dell'introduzione delle più innovative modalità di organizzazione del lavoro, basate sull'utilizzo della flessibilità, sulla valutazione per obiettivi, sulla rilevazione dei bisogni del personale dipendente, il tutto, come già rilevato, alla luce dei bisogni di conciliazione dei tempi di vita e di lavoro[52].

Alcuni vantaggi per i lavoratori sono difficilmente confutabili, primo fra tutti la conciliazione tra tempi di vita e di lavoro. Lavorando da casa, infatti, si riesce a gestire meglio il proprio ritmo di lavoro, valorizzando il tempo a disposizione e abbattendo i costi legati agli spostamenti. L'introduzione dello *smart working*, impattando sul benessere e sulla qualità della vita dei propri dipendenti, può essere considerata una misura di welfare aziendale e si riflette in positivo anche sulla produttività. Vi sono poi altri aspetti di profonda innovazione che vanno evidenziati, sia per i lavoratori che per le amministrazioni, come, ad esempio, la valorizzazione delle risorse umane e una maggiore responsabilizzazione. Altri effetti positivi del lavoro agile possono essere individuati nel fatto che ci si concentra sui risultati del lavoro e non sugli aspetti formali, ma anche: nella razionalizzazione nell'uso delle risorse e sull'aumento della produttività, quindi risparmio in termini di costi e miglioramento dei servizi offerti; nella promozione dell'uso delle tecnologie digitali più innovative e l'utilizzo dello *smart working* come leva per la trasformazione digitale e per lo sviluppo delle conoscenze digitali; nel rafforzamento dei sistemi di misurazione e valutazione delle performance basate sui risultati e sui livelli di servizio; nell'abbattimento delle differenze di genere; nella riduzione delle forme di "assenteismo fisiologico".

In questo scenario, la tecnologia riveste un ruolo di primaria importanza. *smart working* e trasformazione digitale si abilitano vicendevolmente: da una parte, infatti, lo *smart working* ha bisogno delle tecnologie per rendere concrete le sue pratiche e i suoi modelli, dall'altra rappresenta esso stesso una grande leva per la realizzazione della pubblica amministrazione digitale.

Il 12 maggio 2020 *Twitter* ha annunciato: "(..) if our employees are in a role and situation that enables them to work from home and they want to continue to do so forever, we will make that happen". In pratica: cari dipendenti, se lo volete, potete scegliere di lavorare da casa per sempre.

Per far sì che le nuove tecnologie rappresentino un fattore di progresso, e non di regressione sociale, valorizzando, invece di comprimere, le libertà affermate sul terreno gius-lavoristico, è assolutamente

[52] L'art. 14 della legge 7 agosto 2015, n. 124, stabilisce che le amministrazioni adottino misure tali da permettere, entro tre anni, ad almeno il 10% delle lavoratrici e dei lavoratori pubblici che lo richiedano di avvalersi delle nuove modalità di lavoro agile, mantenendo in ogni caso inalterate le opportunità di crescita e di carriera per questi lavoratori.
Viene anche precisato che l'adozione di queste misure organizzative e il raggiungimento degli obiettivi descritti costituiscono oggetto di valutazione nell'ambito dei percorsi di misurazione della performance sia organizzativa che individuale all'interno di ogni ente.

indispensabile garantirne la sostenibilità sotto il profilo costituzionale, democratico e la conformità ad alcuni principi irrinunciabili. Pertanto, il ricorso alle tecnologie ICT per rendere la prestazione lavorativa non deve essere l'occasione per il monitoraggio sistematico e ubiquitario del lavoratore, ma deve avvenire nel rigoroso rispetto delle disposizioni contemplate nello Statuto dei lavoratori, a tutela dell'autodeterminazione del lavoratore, che presuppone un'adeguata formazione e informazione di quest'ultimo. Ponendo in particolare risalto il vincolo finalistico all'attività lavorativa che legittima l'esenzione dalla procedura concertativa o autorizzativa circa gli eventuali controlli mediante strumenti utilizzati per rendere la prestazione lavorativa.

Dopo svariati interventi del Governo, nel corso degli ultimi due anni, riguardanti lo *smart working*, con il decreto legge "Proroghe" del 30 aprile 2021 (G.U. Serie Generale n.103 del 30-04-2021) è stata cancellata la soglia minima del 50% per lo *smart working* nella pubblica amministrazione. Fino alla definizione della disciplina del lavoro agile nei contratti collettivi del pubblico impiego, e comunque non oltre il 31 dicembre 2021, le amministrazioni pubbliche potranno continuare a ricorrere alle modalità semplificate relative al lavoro agile, ma sono liberate da ogni rigidità. Al riguardo, il ministro per la pubblica amministrazione, Renato Brunetta, ha precisato: "Facciamo tesoro della sperimentazione indotta dalla pandemia e del prezioso lavoro svolto dalla ministra Dadone - sottolinea il ministro - per introdurre da un lato la flessibilità coerente con la fase di riavvio delle attività produttive e commerciali che stiamo vivendo e dall'altro lato la piena autonomia organizzativa degli uffici. Fino a dicembre le amministrazioni potranno ricorrere allo *smart working* a condizione che assicurino la regolarità, la continuità e l'efficienza dei servizi rivolti a cittadini e imprese. Un percorso di ritorno alla normalità, in piena sicurezza, concordato con il Comitato tecnico-scientifico e compatibile con le esigenze del sistema dei trasporti". A regime, dall'inizio del 2022, la norma conferma l'obbligo per le amministrazioni di adottare i Pola (Piani organizzativi del lavoro agile) entro il 31 gennaio di ogni anno, riducendo però dal 60% al 15%, per le attività che possono essere svolte in modalità agile, la quota minima dei dipendenti che potrà avvalersi dello smart working. Il "decreto proroghe", come sintetizzato in una nota del Ministro per la Pubblica Amministrazione, prevede che: il lavoro agile non sia più ancorato a una percentuale (soglia del 50% prima prevista), ma al rispetto di principi di efficienza, efficacia e *customer satisfaction*; sia mantenuto inalterato il necessario rispetto delle misure di contenimento del fenomeno epidemiologico e della tutela della salute adottate dalle autorità competenti; si proceda al rinvio alla contrattazione collettiva circa la definizione degli istituti del lavoro agile, ma ne consente fino al 31 dicembre 2021 l'accesso attraverso le modalità semplificate di cui all'art. 87 del decreto legge n. 18 del 2020 (quindi senza la necessità del previo accordo individuale e senza gli oneri informativi a carico della parte datoriale). In caso di mancata adozione del Pola, il lavoro agile sarà svolto da almeno il 15% del personale che ne faccia richiesta. Inoltre, consente implicitamente alle amministrazioni che entro il 31 gennaio 2021 avranno adottato il Pola, con le percentuali previste a legislazione allora vigente, di modificare il piano alla luce della disciplina sopravvenuta. Con Decreto del Presidente del Consiglio dei Ministri del 23 settembre 2021 viene stabilito che dal 15 ottobre 2021 la modalità ordinaria di svolgimento della prestazione lavorativa nella pubblica amministrazione torna ad essere quella in presenza. Si torna, pertanto, al regime previgente all'epidemia pandemica, disciplinato dalla legge 22 maggio 2017, n. 81, recante "Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato" (la legge Madia), così come modificata dai successivi provvedimenti normativi. Spetterà alle singole amministrazioni definire l'organizzazione degli uffici. Nel frattempo, sono in corso le trattative per i rinnovi dei contratti pubblici, che garantiranno, una volta concluse, una regolazione puntuale dello *smart working*. Il Piano integrato della pubblica amministrazione (PIAO, introdotto dal decreto legge 80/2021) assorbirà i contenuti dei Piani organizzativi del lavoro agile (POLA) e rappresenterà per tutte le pubbliche amministrazioni, a partire dal 31 gennaio 2022, uno strumento di semplificazione e di pianificazione delle attività e delle strategie da attuare. Le premesse per il DPCM del 23

settembre 2021 – che mette quindi la parola "fine" all'utilizzo del lavoro agile quale strumento di contrasto al fenomeno epidemiologico e stabilisce che, a decorrere dal 15 ottobre 2021, la modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni è soltanto quella svolta in presenza – sono state poste dal decreto legge 21 settembre 2021, n. 127, con cui il Governo ha esteso a tutto il personale delle pubbliche amministrazioni l'obbligo di possedere e di esibire, per l'accesso al luogo di lavoro, la certificazione verde COVID-19 (il c.d. *green pass*).

Con il decreto legge dell'8 ottobre 2021, n. 139, in attuazione delle disposizioni contenute nel DPCM del 23 settembre 2021, sono state indicate le modalità organizzative per gestire il rientro in presenza del personale dipendente a partire dal 15 ottobre 2021. Il decreto stabilisce che ciascun ufficio è tenuto ad adottare le misure organizzative necessarie per consentire il graduale rientro in sede di tutto il personale in servizio a decorrere dal 15 ottobre ed entro il 31 ottobre, assicurando, da subito la presenza in servizio dei dipendenti preposti alle attività di sportello e ricevimento degli utenti (front office) e di quelli assegnati ai settori preposti all'erogazione di servizi all'utenza (back office), anche attraverso la flessibilità degli orari di sportello e di ricevimento, flessibilità da definirsi previa intesa con le organizzazioni sindacali. L'art. 1, comma 3, del decreto 8 ottobre 2021, nel precisare che "il lavoro agile non è più una modalità ordinaria di svolgimento della prestazione lavorativa", ha disposto, "nelle more della definizione degli istituti del rapporto di lavoro connessi al lavoro agile da parte della contrattazione collettiva e della definizione delle modalità e degli obiettivi del lavoro agile da definirsi (…) nell'ambito del Piano integrato di attività e organizzazione (PIAO)", che l'accesso al lavoro agile possa essere comunque autorizzato nel rispetto di alcune condizioni: "a) lo svolgimento della prestazione di lavoro in modalità agile non deve in alcun modo pregiudicare o ridurre la fruizione dei servizi a favore degli utenti; b) l'amministrazione deve garantire un'adeguata rotazione del personale che può prestare lavoro in modalità agile, dovendo essere prevalente, per ciascun lavoratore, l'esecuzione della prestazione in presenza; c) l'amministrazione mette in atto ogni adempimento al fine di dotarsi di una piattaforma digitale o di un *cloud* o comunque di strumenti tecnologici idonei a garantire la più assoluta riservatezza dei dati e delle informazioni che vengono trattate dal lavoratore nello svolgimento della prestazione in modalità agile; d) l'amministrazione deve aver previsto un piano di smaltimento del lavoro arretrato, ove sia stato accumulato; e) l'amministrazione, inoltre, mette in atto ogni adempimento al fine di fornire al personale dipendente apparati digitali e tecnologici adeguati alla prestazione di lavoro richiesta; f) l'accordo individuale di cui all'art. 18, comma 1, della legge 22 maggio 2017, n. 81, deve definire, almeno: 1) gli specifici obiettivi della prestazione resa in modalità agile; 2) le modalità e i tempi di esecuzione della prestazione e della disconnessione del lavoratore dagli apparati di lavoro, nonché eventuali fasce di contattabilità; 3) le modalità e i criteri di misurazione della prestazione medesima, anche ai fini del proseguimento della modalità della prestazione lavorativa in modalità agile; g) le amministrazioni assicurano il prevalente svolgimento in presenza della prestazione lavorativa dei soggetti titolari di funzioni di coordinamento e controllo, dei dirigenti e dei responsabili dei procedimenti amministrativi; h) le amministrazioni prevedono, ove le misure di carattere sanitario lo richiedano, la rotazione del personale impiegato in presenza, nel rispetto di quanto stabilito dal presente articolo. Al riguardo, il Ministro per la Pubblica amministrazione, il 31 novembre 2021, ha pubblicato lo schema di "Linee guida per *lo smart working* nella Pubblica amministrazione", che anticipano ciò che sarà definito entro l'anno nei contratti di lavoro.

Il 24 marzo 2022 il Governo ha adottato il decreto legge n. 24 (c.d. decreto riaperture), recante "Misure urgenti per il superamento delle misure di contrasto alla diffusione dell'epidemia da COVID-19, in conseguenza della cessazione dello stato di emergenza". Il provvedimento governativo stabilisce, con decorrenza 1° aprile 2022, la cessazione dello stato di emergenza da Covid-19 e introduce misure per il graduale ritorno alla normalità in tutti i settori. Ritorno alla normalità significa l'obbligo per le amministrazioni pubbliche di rispettare la disciplina dettata dalla legge n. 81/2017.

Il decreto legge 80/2021 all'art. 6, comma 6, (convertito dalla legge 6 agosto 2021, n. 113) introduce il nuovo "Piano Unico" della

Pubblica Amministrazione, il "Piano Integrato di Attività e Organizzazione", che deve accorpare, tra gli altri, i piani della performance, del lavoro agile, della parità di genere, dell'anticorruzione. I POLA confluiranno quindi in questo nuovo Piano unico, che avrà durata triennale con aggiornamento annuale e dovrà essere pubblicato dalle amministrazioni entro il 31 dicembre di ogni anno.

L'emergenza sanitaria, determinata dalla pandemia da Sars-CoV-2, è stata per lo *smart working* un importante trampolino di lancio nel nostro Paese[53]; anche se questo innovativo istituto è stato introdotto dal legislatore a partire dal 2017, per lungo tempo esso ha rappresentato uno strumento di nicchia. Nel corso dell'esplosione della pandemia, il ricorso allo strumento dello *smart working* ha garantito la continuità operativa del Paese e, al termine dello stato emergenziale, il c.d. lavoro agile potrebbe imporsi come soluzione funzionale e stabile a un nuovo e più sostenibile equilibrio socio-economico. Se lo stato di emergenza ha permesso al lavoro agile di farsi conoscere ai tanti che ne ignoravano l'esistenza e le potenzialità, ha anche temporaneamente mutato l'istituto sia nella forma (rendendolo semplificato), sia nelle finalità (rendendolo strumento anti-contagio). Nella succitata normativa si ribadisce, anche per la pubblica amministrazione, la centrale importanza nello *smart working* della fissazione degli obiettivi e della valutazione delle performance e dei risultati raggiunti. Con l'istituto in questione si passa dalla misurazione del tempo lavorativo e della presenza in ufficio alla valutazione dei risultati raggiunti.

La legge n. 81/2017, come già ricordato, ha introdotto per la prima volta in Italia una formale regolamentazione del fenomeno dello *smart working*: modalità di esecuzione del rapporto di lavoro subordinato volta a "agevolare la conciliazione dei tempi di vita e di lavoro" e in virtù della quale le prestazioni possono essere rese "in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale" (art. 18, comma 1). Tuttavia, il quadro normativo di riferimento è generale: da un lato non fornisce alcuna prescrizione in materia di protezione dei dati personali, limitandosi (all'art. 21) a un rinvio alle previsioni di cui all'art. 4 Statuto dei Lavoratori e, dall'altro rimanda a un accordo fra le parti la disciplina degli aspetti più rilevanti. Mutando le condizioni logistiche e strumentali della prestazione lavorativa occorre tener conto che cambia necessariamente anche il contesto in cui occorre garantire la protezione dei dati. Per tale motivo, all'improvvisazione iniziale occorre, ora, dare spazio alle regole.

La normativa in materia di protezione dei dati personali non può essere vista come un ostacolo, essa, infatti, presenta istituti di flessibilità per eventi eccezionali, senza che ciò comporti la sospensione dei diritti civili. L'unica nazione europea che ha sospeso, in nome dell'epidemia i diritti dell'interessato (artt. 15-22 del RGPD) è stata l'Ungheria. La pandemia può, infatti, rappresentare il pretesto per introdurre e rafforzare forme di autoritarismo. "Que la pandemia no sea un pretexto para el autoritarismo", che la pandemia non sia un pretesto per l'autoritarismo. Questo è il titolo del "Manifesto", che vede come primo firmatario il premio Nobel per la letteratura Mario Vargas Llosa, pubblicato sul sito della sua Fundación Internacional para la Libertad (FIL)[54]. "Su entrambe le sponde dell'Atlantico - si legge ancora nel documento - risorgono lo statalismo, l'interventismo e il populismo con un impeto che fa pensare a un cambio di modello lontano dalla democrazia liberale e dall'economia di mercato".

Riuscire a conciliare lo *smart working* con la protezione dei dati personali dei lavoratori e con la sicurezza dei dati trattati fuori dalla sede di lavoro sarà una delle sfide dei prossimi anni. La modalità semplificata di ricorso al lavoro agile, senza l'accordo individuale con i lavoratori, più volte oggetto di proroga, va inserita nell'ambito di una cornice normativa più chiara e certa. Nel corso di questi anni sono stati presentati diversi disegni di legge collegati, in particolare, alla manovra di bilancio per il 2021; tra i tanti, segnalo il disegno intitolato "Disposizioni in materia di lavoro agile nelle pubbliche amministrazioni", tra i punti centrali di questo dovrebbero esserci il diritto del lavoratore alla disconnessione e il potenziamento della

[53] Il Ministro per la Pubblica Amministrazione, con il D.M. 4 novembre 2020, ha anche istituito l'Osservatorio nazionale del lavoro agile nelle amministrazioni pubbliche.

[54] *https://fundacionfileggeorg/*

formazione digitale dei lavoratori delle amministrazioni pubbliche.

Con il passaggio al digitale del mondo del lavoro, le occasioni di controllo a distanza dei lavoratori crescono notevolmente. Ogni nuova tecnologia ICT agevola l'attività lavorativa, ma cela alcuni rilevanti problemi applicativi, nascenti dall'art. 4 dello Statuto dei lavoratori[55].

Il predetto articolo pone dei paletti precisi per l'uso delle nuove tecnologie. La norma vieta l'uso di ogni strumento che consenta il controllo a distanza dei lavoratori, facendo limitate eccezioni per gli "strumenti di lavoro" e gli apparecchi il cui utilizzo sia stato autorizzato da un accordo sindacale o, in assenza, da un provvedimento dell'Ispettorato del lavoro. In questa visione, molti degli strumenti utilizzati dal lavoratore rischiano di entrare in conflitto con il dettato normativo. I limiti che lo Statuto dei lavoratori ha posto al potere organizzativo e, soprattutto, disciplinare del datore di lavoro sono notevoli. Lo scopo, anche dopo la riforma, è quello di salvaguardare la personalità e la dignità del lavoratore e, quindi, la sua integrità fisica e morale anche all'interno dei luoghi di lavoro in applicazione dei principi costituzionali. Il legislatore del *Jobs act* ha voluto riscrivere l'art. 4 dello Statuto[56], con l'intento di renderlo più vicino alla realtà dell'organizzazione dell'impresa. La novella ha fatto venir meno il principio del divieto assoluto e la storica contrapposizione tra il primo e il secondo comma della vecchia formulazione, che negli ultimi anni aveva alimentato le più ampie interpretazioni da parte della giurisprudenza e del Garante per la protezione dei dati personali. Ciò ha consentito al legislatore l'apertura, contenuta nel comma 2 della nuova norma, di grande rilevanza pratica per gli strumenti tecnologici "mobili" (*pc*, *tablet*, *smartphone*, *Gps*, ecc.) che potranno essere utilizzati dai lavoratori anche senza l'accordo con le Rsa/Rsu ovvero senza autorizzazione amministrativa. Ricorrendo una delle esigenze di controllo previste dallo Statuto, il datore di lavoro potrà monitorare lo *smart worker* tramite gli strumenti di lavoro anche al fine di verificare la sua diligenza nell'adempimento dei propri obblighi, con possibili conseguenze sul piano disciplinare. L'ultimo comma dell'art. 4 dello Statuto prevede che le informazioni ottenute "sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal d.lgs. 30 giugno 2003, n. 196", e oggi ancor più alla luce del Regolamento (UE) 2016/679 (*Regolamento Generale sulla Protezione dei Dati* - RGPD). In caso di omissione dell'informativa, il datore di lavoro non solo viola la disciplina in materia di protezione dei dati personali, ma rende anche censurabile qualsiasi atto disciplinare venga emanato sulla base delle informazioni raccolte tramite controllo a distanza.

Il datore di lavoro non può, però, monitorare sistematicamente l'attività del lavoro, il Garante già con le Linee guida del 1° marzo 2007[57] aveva ribadito come l'accesso indiscriminato agli strumenti in dotazione al personale rappresenti un illecito. Il Garante riconosce la facoltà del datore di verificare l'esatto adempimento della prestazione professionale e il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, purché ciò avvenga nel rispetto della libertà e della dignità dei lavorati oggetto di controllo, nonché, in particolare, in ossequio della normativa in materia di protezione dei dati personali. Il Garante (con il provvedimento n. 303/2016) aveva affermato che il ricorso a programmi che operano in *background*, come tali non percepibili dai lavoratori, che permettano una verifica costante e indiscriminata degli accessi degli utenti alla rete e all'e-mail fossero in contrasto con il Codice in materia di protezione dei dati personali e con lo Statuto dei lavoratori. Sempre il Garante, con il provvedimento 547/2016) ribadiva che le modifiche introdotte dal *Jobs act* non permettevano comunque

[55] A. Bellavista, *Il controllo sui lavoratori*, Torino, Giappichelli, 1995.

[56] A. Bellavista, *Il nuovo art. 4 dello Statuto dei lavoratori*, in G. Zilio Grandi e M. Biasi (a cura di), *Commentario breve alla riforma "Jobs Act"*, Padova, Wolters Kluwer, 2016, 717 ss.; E. Barraco, S. Iacobucci, *Strumenti di lavoro e controllo a distanza*, in *Diritto e pratica del lavoro*, 2018, 1942 ss.; M.T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.lgs. 151/2015): spunti per un dibattito*, in *Labour & Law Issues*, 2016, 1 ss.; A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *Rivista italiana di diritto del lavoro*, 2016, 513 ss.

[57] Garante per la protezione dei dati personali, *Lavoro: le linee guida del Garante per posta elettronica e internet*, 1 marzo 2007, in www.garanteprivacy.it, doc. web n. 1387522.

l'effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore.

Qualora legittimi nell'ambito della disciplina lavoristica, i controlli devono avvenire nel rispetto dei principi di trasparenza, minimizzazione, proporzionalità e progressività nel trattamento, così come previsto dall'art. 5 del RGPD.

Con il parere dell'8 giugno 2017, il Gruppo di lavoro ex art. 29 ("WP29"), ora Comitato europeo per la protezione dei dati, si è pronunciato in merito al trattamento dei dati personali dei lavoratori, integrando quanto già previsto in passato con il Parere n. 8/2001 ("Parere sul trattamento di dati personali nell'ambito dei rapporti di lavoro") ed il "Documento di lavoro sulla sorveglianza delle comunicazioni elettroniche sul luogo di lavoro" del 2002.

Come precisato dal WP29, tale nuovo parere è finalizzato ad aggiornare le regole per il trattamento dei dati personali dei lavoratori alla luce dell'evoluzione delle tecnologie informatiche (es.: sistemi per il controllo del lavoro da remoto, geolocalizzazione, *Data Loss Prevention*) nonché alla piena operatività del Regolamento UE n. 2016/679.

Nel documento in esame il WP29 ha, dapprima, ricordato che nell'effettuare il trattamento di tale tipologia di dati personali i datori di lavoro devono tenere ben presenti i diritti fondamentali dei lavoratori, ivi incluso il diritto alla loro riservatezza e, successivamente, individuato le basi giuridiche di tale trattamento, precisando che queste ultime possono ravvisarsi, alternativamente: nell'esecuzione di obblighi derivanti da un contratto di lavoro, ove presente (es.: finalità retributive - ai sensi dell'art. 6.1, lett. b) del GDPR); nell'adempimento di obbligazioni previste dalla legge (es.: calcolo della ritenuta d'imposta - ex art. 6.1, lett. c) del GDPR); nell'interesse legittimo del datore di lavoro (es.: prevenzione della perdita di materiali aziendali e/o miglioramento della produttività dei lavoratori - ex art. 6.1, lett. f) del GDPR).

Il WP29, invece, esclude dalle basi giuridiche del trattamento dei dati personali dei lavoratori il mero consenso di questi ultimi in quanto, a causa del rapporto di "dipendenza", e quindi di debolezza, nei confronti del datore di lavoro, lo stesso consenso non potrebbe mai ritenersi liberamente prestato né, per le stesse ragioni, liberamente revocabile.

Con particolare riferimento all'interesse legittimo del datore di lavoro, poi, il WP29 ricorda a ciascun datore di lavoro di valutare preventivamente se il trattamento da porre in essere sia necessario e proporzionato per il perseguimento di una finalità legittima, nonché di mettere in atto idonee misure di sicurezza dirette a bilanciare tale finalità con i diritti e le libertà fondamentali dei lavoratori, redigendo, se necessario, anche una valutazione di impatto del trattamento ai sensi dell'art. 35 del RGPD.

Il WP29 consiglia ai datori di lavoro specifiche misure di sicurezza idonee a prevenire eventuali violazioni della riservatezza degli interessati, tra cui, ad esempio, l'esclusione delle cd. "aree sensibili" (ospedali o luoghi religiosi) dalle zone sottoposte a monitoraggio, il divieto di monitoraggio delle cartelle/dei file e/o delle comunicazioni personali dei dipendenti e/o, ancora, la previsione di un monitoraggio "a campione", rispetto ad una sorveglianza continuata nel tempo (Al riguardo, Garante, provvedimento 24 maggio 2017, n. 24, in www.garanteprivacy.it, doc. web n. 6495708).

Il WP29 ricorda, inoltre, che nel caso in cui il trattamento dei dati dei lavoratori si fondi sull'interesse legittimo del titolare, quest'ultimo è sempre tenuto a garantire agli interessati il diritto di opporsi al trattamento, esercitando l'omonimo diritto loro conferito dall'art. 21 del GDPR.

Mediante il suddetto parere, il WP29 ha individuato 9 scenari tipici di trattamento di dati personali dei lavoratori - per lo più basati su un interesse legittimo del titolare del trattamento - che possono presentare dei rischi per i diritti e le libertà fondamentali di questi ultimi. Per ognuno di tali scenari, il WP29 ha inoltre rammentato che il datore di lavoro deve procedere, nel rispetto dei principi di "privacy by design" e "privacy by default" previsti dal RGPD, alla previa individuazione della base giuridica del trattamento, alla verifica della necessità delle operazioni di trattamento e all'esame della correttezza e proporzionalità dello stesso rispetto alle finalità perseguite: 1) Trattamento dei dati dei candidati presenti sui *social network*; 2) Trattamento dei dati dei lavoratori presenti sui social network; 3) Monitoraggio della strumentazione informatica dei lavoratori; 4) *Mobile Device Management*; 5) *Wearable*

Devices; 6) Rilevazione della presenza dei lavoratori; 7) Trattamenti di dati mediante sistemi di videosorveglianza; 8) Geolocalizzazione dei veicoli; 9) Trasferimento dei dati personali dei lavoratori a terzi.

Mediante il predetto parere il WP29 ha introdotto, alla luce delle nuove tecnologie informatiche ICT e della nuova disciplina introdotta dal GDPR, delle specifiche regole per il trattamento dei dati dei lavoratori.

Tali disposizioni rappresentano un punto di riferimento di particolare importanza per i datori di lavoro che intendono trattare i dati personali dei propri lavoratori, in quanto, da un lato, definiscono le basi giuridiche di tale tipologia di trattamento e, dall'altro, tramite esempi pratici, approfondiscono il generico concetto di "legittimo interesse" del titolare, così come previsto dall'art. 6.1 lett. f) del RGPD. Il parere, inoltre, ricorda ai datori di lavoro di adottare sempre, nel rispetto del principio di "*accountability*" (responsabilizzazione) previsto dal RGPD (in particolare, art. 24), misure preventive volte alla protezione della riservatezza dei lavoratori redigendo, se del caso, anche una valutazione di impatto del trattamento che abbia ad oggetto il bilanciamento tra il proprio legittimo interesse e l'impatto delle nuove tecnologie informatiche utilizzate sui diritti e le libertà fondamentali degli interessati.

Diversi, come già rilevato, sono gli strumenti che potrebbero entrare potenzialmente in conflitto con l'art. 4 dello Statuto. Si pensi, ad esempio, all'utilizzo della video chiamata, diventata il mezzo più comune di gestione della prestazione lavorativa per chi opera in regime di *smart working*. Secondo il succitato art. 4, l'uso può essere lecito sole se questa è fatta rientrare nella nozione di "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", unica categoria per la quale non è richiesta la stipula dell'accordo sindacale o una procedura alternativa di autorizzazione amministrativa. Sul punto, le Autorità di controllo hanno manifestato un approccio più restrittivo alla nozione di strumenti di lavoro. Altro sistema che suscita diffuse perplessità e che ha forti potenzialità di controllo è il meccanismo che avvisa con una sorta di "semaforo" verde, giallo o rosso sulla presenza davanti al pc e sul collegamento alla rete aziendale di un lavoratore. Anche questo programma è di uso comune, ma può entrare in conflitto con l'impianto dell'art. 4, poiché indubbiamente genera un controllo a distanza. In tali casi, occorrerà l'accordo sindacale o l'autorizzazione amministrativa, e sarà necessario valutare la legittimità del trattamento, che non deve tradursi in una forma di monitoraggio, nonché fornire al lavoratore l'informativa, ai sensi dell'art. 13 RGPD, ed eseguire una valutazione d'impatto, ai sensi dell'art. 35 RDPD.

Meno questioni sembra creare l'uso delle chat (tipo *Whatsapp*) per scopi lavorativi, per le quali non servirebbero l'accordo sindacale o l'autorizzazione amministrativa, pur trattandosi di uno strumento potenzialmente invasivo, non pare profilarsi quella forma di controllo a distanza previsto dall'art. 4. Tuttavia, andrebbe sconsigliato l'uso delle chat come *Whatsapp* per finalità lavorative, poiché questo comporta la comunicazione e l'eventuale diffusione di dati e/o documenti che il datore di lavoro avrebbe poi difficoltà a controllare.

Sicuramente più problematica è la questione dell'utilizzo delle c.d. *werable technologies* (ad esempio, occhiali con GPS, braccialetti intelligenti, capi di abbigliamento interattivi) che offrono grandi opportunità di migliorare la qualità del lavoro, ma nello stesso tempo generano opportunità di controllo, per le quali non sarebbe facile far rientrare nella nozione di strumenti di lavoro, anche se la valutazione va compiuta caso per caso. In tali casi, oltre all'accordo sindacale o l'autorizzazione amministrativa, sarebbero necessari l'informativa, ai sensi dell'art. 13 RGPD, la valutazione d'impatto ai sensi dell'art. 35 RGPD e un'attenta analisi sulla possibilità di fondare tali trattamenti su basi giuridiche diverse dal consenso.

Il titolare del trattamento deve tener conto che il principio di *accountability* (responsabilizzazione) rappresenta il principio fondamentale del RGPD e si estende a qualsiasi iniziativa o misura intesa a favorire i trattamenti di dati da svolgersi in modalità *smart working*. Ciò significa che il titolare deve adottare comportamenti proattivi che dimostrino la concreta adozione di misure dirette ad assicurare l'applicazione del RGPD. Il titolare deve decidere in piena autonomia le modalità, le garanzie e i limiti del trattamento dei dati, in ossequio alla normativa in materia di protezione dei dati personali. Al riguardo, come previsto dall'art. 24 RGPD, su tali aspetti dovrà lasciare traccia delle proprie

decisioni anche in relazione allo *smart working*. Particolarmente delicata è la questione della sicurezza dei dati trattati mediante lavoro agile, situazione che rischia di legittimare comportamenti che possono mettere a rischio la conformità dell'azienda o della PA alla normativa in materia di protezione dei dati personali, nonché facilitare una cyber attacco con notevoli conseguenze negative sull'operatività della PA o dell'azienda e ingenti danni economici. Il titolare, oltre a predisporre misure tecniche e di sicurezza idonee atte a mitigare i rischi che gravano sulle attività di trattamento, dovrà integrare il registro dei trattamenti con nuovi elementi (trattamenti, banche dati, strumenti, esternalizzazioni, misure di sicurezza) che dovessero riguardare le attività in *smart working*; valutare, ai sensi del RGPD e dello Statuto dei Lavoratori, il potenziale invasivo di eventuali sistemi che consentano il monitoraggio dell'utilizzo degli strumenti e della rete aziendale, eventualmente sottoponendoli a valutazione d'impatto; valutare la necessità di integrare l'informativa ai lavoratori alla luce di eventuali nuovi trattamenti datoriali connessi allo *smart working*; ricalibrare l'ambito di autorizzazione dello *smart worker*, laddove necessario e applicando in maniera maggiormente restrittiva il principio di *need to know*; integrare/riformulare, in funzione del contesto delocalizzato, le istruzioni per la sicurezza dei dati da rendersi allo *smart worker*; avviare specifiche iniziative di formazione per conferire al lavoratore agile gli opportuni strumenti di conoscenza e consapevolezza; verificare che le soluzioni informatiche eventualmente sviluppate internamente, per consentire lo svolgimento del lavoro a distanza, siano conformi ai principi di *privacy by design*/*by default* e garantiscano la sicurezza dei dati ex art. 32 RGPD; verificare la contrattualistica e la conformità al RGPD delle soluzioni o piattaforme fornite da terzi, valutando la necessità/adeguatezza di eventuali *data processing agreement* da sottoscrivere ai sensi dell'art. 28 del RGPD. Le predette attività, in gran parte strettamente connesse tra loro, dovranno essere prodotte adottando una metodologia e un piano di azione dalla logica sincretica e coordinata.

Gli strumenti utilizzati dallo *smart worker* per prestare la propria attività lavorativa consentono una reperibilità e una connessione costante e continua. Ciò rischierebbe di compromettere il bilanciamento tra vita professionale e vita privata che è tra i presupposti dell'istituto del lavoro agile. In tale quadro si inserisce il diritto alla disconnessione, in virtù del quale il prestatore di lavoro deve essere protetto da una potenziale perenne connessione.

La flessibilità oraria e organizzativa, offerta dalle nuove tecnologie ICT in ambito lavorativo, da una parte può rappresentare un'importante opportunità per conciliare vita e lavoro, dall'altra rischia di accentuare il conflitto tra vita privata e vita lavorativa e dar luogo a quel fenomeno definito "time porosity", che indica i confini sfumati tra tempi di vita e tempi di lavoro[58]. La connessione ininterrotta fa sì che il lavoratore possa essere sempre contattato, essendo esposto "a uno stato permanente di allerta reattiva rispetto al soddisfacimento delle richieste datoriali"[59]. In tale contesto, è cominciata a emergere l'esigenza di tutelare la disconnessione, secondo la quale il lavoratore deve essere protetto da una potenziale perenne connessione, ossia una tutela diretta a individuare strumenti e modalità, con i quali lo *smart worker* possa interrompere i contatti, senza che ciò determini ripercussioni sul piano retributivo o venga a incidere sul corretto adempimento della prestazione lavorativa.

Nella legge n. 81/2017, la disconnessione viene riconosciuta, seppur senza fornire una definizione giuridica, all'art. 19, comma 1, il quale prevede che l'accordo sullo *smart working* debba contenere, oltre ai tempi di riposo del lavoratore, anche le "misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro". Nel contesto del diritto alla disconnessione, dunque, il prestatore di lavoro deve, in sostanza, essere libero di disattivare le strumentazioni tecnologiche e le piattaforme informatiche di lavoro. Nell'accordo individuale, sottoscritto dal datore di lavoro e dal lavoratore, devono, quindi, essere previsti i tempi di riposo e le misure tecniche ed organizzative cosicché il lavoratore possa interrompere i collegamenti informatici e disattivare i dispositivi elettronici sulla base

[58] R. Zucaro, *Il diritto alla disconnessione tra interesse collettivo e individuale. Possibili profili di tutela*, in *Law & Labour Issues*, 2019, 1 ss.

[59] D. Poletti, *Il diritto alla disconnessione nel contesto dei "diritti digitali",* in *Responsabilità civile e previdenza*, 2017, 1 ss.

delle prescrizioni ivi inserite. Essendo in presenza di una norma imperativa che necessita dell'eterointegrazione da parte della contrattazione collettiva, successivamente all'entrata in vigore della legge n. 81/207, infatti, il diritto alla disconnessione è stato espressamente disciplinato, nel pubblico, dal CCNL relativo al personale del comparto Istruzione e Ricerca 2016/2018, firmato il 18 aprile 2018. L'art. 22, comma 4, lett. C8), del CCNL in questione rinvia alla contrattazione integrativa la definizione di "criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio al fine di una maggiore conciliazione tra vita lavorativa e familiare (diritto alla disconnessione)".

Il D.M. del Ministro per la Pubblica Amministrazione del 19 ottobre 2020, all'art. 5, ha previsto che: "1. Il lavoro agile si svolge ordinariamente in assenza di precisi vincoli di orario e di luogo di lavoro. 2. In ragione della natura delle attività svolte dal dipendente o di puntuali esigenze organizzative individuate dal dirigente, il lavoro agile può essere organizzato per specifiche fasce di contattabilità. 3. Nei casi di prestazione lavorativa in modalità agile, svolta senza l'individuazione di fasce di contattabilità, al lavoratore sono garantiti i tempi di riposo e la disconnessione dalle strumentazioni tecnologiche di lavoro".

Nel corso di un'audizione in Parlamento, il 13 maggio 2020, il Garante per la protezione dei dati personali ha affermato con forza che è necessario assicurare in "modo più netto" il diritto alla disconnessione per tutelare la distanza tra spazi di vita privata e attività lavorativa ("una delle più antiche conquiste" in fatto di diritti sul lavoro. "Il ricorso alle tecnologie – ha aggiunto il Presidente del Garante – non può rappresentare l'occasione per il monitoraggio sistematico del lavoratore. Deve avvenire nel rispetto delle garanzie sancite dallo Statuto a tutela dell'autodeterminazione del lavoratore che presuppone, anzitutto formazione e informazione del lavoratore sul trattamento a cui i suoi dati saranno soggetti". "Non sarebbe legittimo fornire per lo *smart working* un computer dotato di funzionalità che consentono al datore di lavoro di esercitare un monitoraggio sistematico e pervasivo dell'attività compiuta dal dipendente tramite questo dispositivo". Pertanto, la disconnessione darebbe luogo a un nuovo diritto digitale, che si connoterebbe come un corollario del diritto alla privacy[60], in particolare come "diritto di essere lasciato in pace", come diritto alla tranquillità individuale.

[60] D. Poletti, *Il diritto alla disconnessione*, 17.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 117-131
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 09

*AI Systems in the Public Sector: Risks and Its Answers Within the EU Data Protection Framework**

Genoveva Gil García

(Tech-lawyer and data protection specialist working at Serendipity Holding B.V (Eindhoven, The Netherlands) and former Blue Book trainee at the Data Protection Office of the European Commission. She holds an LL.M in Law and Technology from Tilburg University, The Netherlands)

ABSTRACT In this paper the author analyses the risks posed by AI systems and the solutions already offered by the existing Data Protection Framework in the EU. In this regard, algorithmic risk-assessment tools are taken as case studies throughout the contribution. The analysis, although focused on Data Protection law, addresses the proposal for an AI act and takes into consideration the technicalities of AI systems. The paper concludes with some recommendations to be considered when implementing this new technology in our society, and especially in the public sector.

1. *Introduction*

The use of artificial intelligence is becoming more and more widespread in different sectors of society, including the public sector. For instance, there are already some discussions regarding the possibility of AI replacing judges or lawyers ('robot judges' or 'robot lawyers'), the use of AI as an assistance in the practice of law, the use of AI in job-recruitment processes[1] or even in the health sector.[2] These are just a few examples where the family of decision-making AI systems can be found.

Decision-making AI systems are designed to help in decision-making processes by mainly using automated data processing and machine-learning techniques. These self-learning AI systems make predictions or reach decisions by analysing large amounts of data and identifying patterns within datasets.[3] In particular, a great part of these tools conducts risk profiling by ranking individuals or groups, using correlations and probabilities drawn from the analysis of Big Data, to determine the level of risk of a certain event to occur.[4] Some examples can also be seen in the fintech sector, where the tools profile users into risk categories before providing financial advice;[5] in the insurance sector, where some models for assessing the risks of insurance companies' functioning have been explored;[6] in the context of criminal proceedings, to aid judges in the decision-making process, but also to grant prison privileges;[7] for unemployed profiling at public administration level;[8] or in the detection of tax fraud, where some of these tools have already been tested by some jurisdictions in the EU (e.g., Poland and the Netherlands).[9]

* Article submitted to double-blind peer review.

[1] For instance, *Pure Matching* is a recruitment matching AI system created by a software company in the Netherlands which promises to match available vacancies and jobseekers. See www.purematching.com/how-it-works accessed 17 April 2023.

[2] See C. Habib et al., *Health Risk Assessment and Decision-Making for Patient Monitoring and Decision-support using Wireless Body Sensor Networks*, in *Information Fusion*, vol. 47, 2018, 10-22.

[3] Committee of experts on internet intermediaries of the Council of Europe, Algorithms and human rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, 2018, 6-7.

[4] See S. van Schendel, *Risk Profiling by Law Enforcement Agencies in the Big Data Era: Is There a Need for Transparency?*, in E. Kosta et al. (eds.), *Privacy and Identity Management: Fairness, Accountability and Transparency in the Age of Big Data*, Springer, 2018, 275-289.

[5] See S. Krishnan, S. Deo and N. Sontakke, *Operationalizing algorithmic explainability in the context of risk profiling done by robo financial advisory apps*, in *Data Governance Network*, 2020.

[6] See O. Kozmenko and V. Oliyniyk, *Statistical model of risk assessment of insurance company's functionaning*, in *Investment Management and Financial Innovations*, vol. 12, 2015, 189-194.

[7] For instance, RisCanvi is currently being used in Catalonia (Spain) to estimate the risk that inmates reoffend when deciding whether or not to allow for parole. However, the system was not subject to any impact assessment and there is little transparency about it. (N. Bellio López-Molina, *In Catalonia, the RisCanvi algorithm helps decide whether inmates are paroled*, 2021).

[8] Joint Research Centre (European Commission), AI Watch. Artificial Intelligence in public services. Overview of the use and impact of AI in public services in the EU, Brussels, 2020, 46.

[9] See M. Papis-Almansa, *The Polish Clearing House System: A 'Stir'ing Example of the Use of New Technologies in Ensuring VAT Compliance in Poland and*

Indeed, in 2014, the Dutch government launched SyRi (*Systeem Risico Indicatie*), a tool which aimed to detect different forms of fraud, including social benefits, allowances, and tax fraud. The Dutch Tax Authority penalised families over a suspicion of fraud based on the risk scores provided by this AI risk-assessment tool. Many households – usually belonging to ethnic minorities or families with lower incomes– fell into poverty given the high amount of the fines imposed by the authority due to a wrong risk indicator. To date, a great part of them is still suffering from the economic consequences.[10] However, in February 2020, the Hague District Court ruled that the legislation regulating the use of SyRi, violates Article 8 of the European Convention on Human Rights (hereafter ECHR). The Court stressed that the application of SyRi was "*insufficiently transparent and verifiable*", and the authorities ceased to use this tool.[11]

This case illustrates that this new technology poses challenges to society and hence the need to address them. Therefore, it is necessary to define how to shape these tools in order to reap the benefits while protecting individuals rights and freedoms. In this regard, there is a need for an in-depth analysis of this topic from the perspective of the right to privacy and data protection since the processing of personal data is inherent to the nature of this technology.

Consequently, in this contribution, the author will try to briefly identify the risks posed by this new technology to individuals' fundamental rights and hence the challenges that lie ahead for (but not exclusively) public administrations. From there, it will be possible to explain how the instruments offered by the existing data-protection framework can help mitigate some of the risks presented by this technology, and how this can be translated into some considerations or recommendations for the implementation and use of AI systems by public administrations. The author will illustrate the latter by referring to some examples found in the public sector.

In the current legislative context, this analysis becomes even more important, due to the Proposal for a Regulation of Artificial Intelligence (hereafter AI act) of the European Commission of the 21 April 2021,[12] the recent Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence published on the 28 September 2022,[13] or the opening of negotiations for a Council of Europe Convention on Artificial Intelligence.[14] The proposal for an AI act establishes the requirements that providers and users of AI systems will need to fulfil in order to place them in the market or to put them into service. It follows a risk-based approach defining clear requirements for high-risk AI systems. Indeed, a tool like SyRi would be considered a high-risk AI system according to Article 5 of Annex III of the Proposal.[15] It remains to be seen what the final text of the Proposal will be, but the act is being widely debated not only by civil society organisations, tech lawyers and scholarship, but also in the European Parliament and the Council in accordance with the ordinary legislative procedure.

With regard to the methodology, the author will approach the topic from an EU perspective. For this, legal and non-legal scholarship will be useful to gain some insight into the topic as well as to identify potential risks and possible solutions to mitigate them. The study of already-existing examples of risk-assessment tools (e.g., SyRi), will be taken into consideration. This will help the author to get familiar with this technology and to identify the risks and answers to the challenges.

The use of European policy documents will

Selected Legal Challenges, in *EC Tax Review*, vol. 28, 2019, 43-56; and S. van Schendel, *The challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRi, in Regulating New Technologies*, in L. Reins (ed.), *Uncertain Times*, The Hague, 225-240.

[10] See *Dutch scandal serves as a warning for Europe over risks of using algorithms* www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/ accessed 24 October 2022.

[11] The Hague District Court, C/09/550982/HA ZA 18-388 Judgment of 5 February 2020 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 accessed 17 April 2023.

[12] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, Brussels, 2021.

[13] European Commission, *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)*, Brussels, 2022.

[14] European Commission, *Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy, and the rule of law*, Brussels, 2022.

[15] European Commission, *Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, Brussels, 2021.

be required to describe the current views of different European institutions on the topic. In this regard, not only will the papers issued by the European Union be looked into, but also the ones from the Council of Europe. Indeed, in order to propose possible solutions, the Ethics Guidelines for Trustworthy AI will be a helpful starting point to rely on, as it sets out the principles that the use of AI should respect.[16] As indicated, European data-protection law will also be of utmost relevance due to the vast amount of personal data usually processed by these tools. Furthermore, the proposal for an AI act will be briefly addressed since it contains the requirements that high-risk AI systems will have to comply with.

2. *AI systems, machine learning and risks of algorithmic risk-assessment tools*

2.1. *Introduction*

There is no common definition for "artificial intelligence", "algorithms" or "AI systems". However, the European Union Agency for Fundamental Rights (hereafter FRA) defines 'algorithms' as "a sequence of commands for a computer to transform an input into an output".[17] To put it simple, algorithms are part of so-called AI systems, which the Commission in the Proposal for an AI act has defined as: "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". This definition, among quite a few other aspects, is currently being debated in the Parliament and the Council.

A great majority of AI systems make use of machine-learning techniques, which means that they 'learn' by analysing large amounts of data in order to establish correlations within datasets. Hence, machine learning is a necessary component of AI system models and AI.

As indicated in the Introduction of this paper, a great part of decision-making AI systems makes use of these techniques to conduct risk profiling and to reach a decision according to the risk score concluded by the system. This specific type of AI systems is the subject of this contribution, and it is referred to as algorithmic risk assessment tools.

Machine-learning AI systems require at least three different types of datasets to produce a certain outcome: training data, input data and inferred labels.[18] Training data are used to build the model. Input data are the information introduced into the AI system to achieve the desired output. Finally, the system finds correlations between the training and input data, and it produces an inferred label. In the case of SyRi, due to its lack of transparency it was not clear whether it made use of machine-learning techniques or not. Actually, the Court of The Hague noted that the State did not disclose the risk model and the indicators composing the tool .[19] However, if the tool would have followed the latter structure, training data would be constituted by historical data of former fraudsters; input data would be potential fraudsters' personal data; and the output would be a risk score based on a correlation between the two data sets.

This process shows the great influence and importance that data quality has in risk profiling conducted by the tool. If training data are of low quality or contain biases, it may lead to inaccurate outputs which could infringe fundamental rights, like the right to non-discrimination or the right to privacy and data protection.[20]

On another note, machine-learning AI systems are commonly known as 'black boxes'. However, this claim does not respond to all different models in which AI systems can be presented. For the purposes of this paper, machine-learning AI systems can be divided into interpretable models and deep-learning models. Interpretable models (e.g., decision trees) provide transparency and allow human users to trace the steps taken by the tool in the decision-making process. Deep-learning models (e.g., neural networks) are considered 'black boxes' either because their complicated structure and functioning are

[16] High-Level Expert Group on Artificial Intelligence of the European Commission, *Ethics Guidelines for Trustworthy AI*, 2019.

[17] European Union Agency for Fundamental Rights, *#BigData: Discrimination in data-supported decision making*, Vienna, 2018, 4.

[18] European Union Agency for Fundamental Rights, *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, Vienna, 2019, 4-5.

[19] The Hague District Court, C/09/550982/HA ZA 18-388 Judgment of 5 February 2020 paragraph 6.49 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 accessed 17 April 2023.

[20] European Union Agency for Fundamental Rights, *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, 5.

uninterpretable to human users, or because only a few experts are capable to understand the machine codes.[21] In addition, sometimes the opacity is not only due to technical reasons, but because the tool contains proprietary know-how and hence it is protected by intellectual property rights. This is why it is widely said that 'black-box' algorithms cause a lack of transparency or explainability in the decision-making process.[22] There is a clear risk here for the right to data protection. According to Data-protection legislation, the data subject has the right to know what personal data and the way in which data are processed. Equally, in the case of SyRi, individuals should have also been provided with this information in order to be able to challenge the decision adopted by the tool.

In this same regard, in 2012 the Polish Ministry of Labour and Social Policy implemented an automated profiling system for unemployment. This system divided unemployed persons in three categories to determine the type of program they were eligible for. However, in this case citizens were informed neither of the score received, nor of how the tool reached this result. The tool was ruled unconstitutional by the Polish Constitutional Tribunal in 2019.[23]

In addition to the above, algorithmic risk-assessment tools make use of automated decision-making systems (hereafter ADMSs). ADMSs can be used to produce outcomes without human intervention, meaning that the decision would be fully automated; or to serve as a tool for humans in their decision-making process. In principle, the results provided by these tools should be considered as a mere instrument to aid the reviewer of a case during an investigation or procedure. However, the automation element will still be present and there is a risk of human reviewers being partial.

To conclude this section, by describing the tool it is possible to briefly identify the main risks that the use of AI risk assessment tools entails. These risks are essentially: risk of discrimination, risk of AI systems' opacity and the risk of falling into automation. The following sections will provide a more extensive description of them.

2.2. *The risks of algorithmic risk-assessment tools*

2.2.1. *Risk of discrimination*

Algorithmic risk-assessment tools are machines controlled and designed by humans. Consequently, the choices about data made by their designers will necessarily have an impact on the tool's prediction. These tools are trained on historical data and hence there is a risk of perpetuating and reinforcing historical biases or prejudices, which could lead to discriminatory outcomes.[24] This result would be contrary to the principle of fairness stated by the High-Level Expert Group on AI. According to this group, an AI system is fair if it is free from bias, discrimination, and stigmatisation.[25]

It is worth mentioning the distinction between direct and indirect discrimination provided by the Council of Europe in the context of ADMSs. Direct discrimination occurs when the decision about an individual is directly based on protected grounds such as race, ethnicity, or gender. Since these unfair biases are usually made sub-consciously, it is said that AI systems can exclude those biases. Indirect discrimination arises when a certain factor occurs more frequently among the groups against whom it is unlawful to discriminate. In this case, certain individuals are treated differently because the decision relies on biased data.[26]

For instance, this is the kind of discrimination which has been claimed in the case of COMPAS, a tool used by US courts to assess defendants' risk of recidivism when judges must determine the sentence for an individual.[27] This tool raised concerns about

[21] A. Rai, *Explainable AI: from black box to glass box*, in *Journal of the Academy of Marketing Science*, vol. 48, 2020, 138.

[22] Council of Bars and Law Societies of Europe, *Considerations on the legal aspects of artificial intelligence*, CCBE, 2020, 12.

[23] Joint Research Centre (European Commission), *AI Watch. Artificial Intelligence in public services. Overview of the use and impact of AI in public services in the EU*, Brussels, 2020, 46-47.

[24] L. Edwards and M. Veale, *Enslaving the Algorithm: From a "Right to and Explanation" to a "Right to Better Decisions"?*, in *IEEE Security & Privacy*, vol. 16, 2018, 46.

[25] High-Level Expert Group on Artificial Intelligence of the European Commission, *Ethics Guidelines for Trustworthy AI*, 2019, 12.

[26] Committee of experts on internet intermediaries of the Council of Europe, *Algorithms and human rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, 2018, 26-27.

[27] See Partnership on AI, Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System, 2019; Thomas Blomberg et al., *Validation of the COMPAS risk assessment classification instrument*, in *Centre for Criminology and Public Policy Research*

its fairness for being based on factors that seem biased, such as racial bias or gender bias.[28] In the case of SyRi, having dual nationality was connected to "low income" and interpreted as a risk indicator.[29] Similarly, the Polish unemployment tool assessed women in a different way than men, and the distinction lowered their chances to receive assistance from public authorities.[30]

The challenges to correctly design risk-assessment tools can be divided in two. First, the selection of the data that will be embedded into the machine. Second, the detection and avoidance of possible miscodes or errors that the AI system may fall into during the decision-making process.[31]

With regard to the first challenge, the quality of the data to feed the AI system is crucial to avoid the risk of discrimination. In this vein, the FRA highlights two sources of error when selecting the data: measurement errors and representation errors. Measurement error refers to "how accurately the data used indicate or reflect what is intended to be measured". For instance, if there is an intention to measure the country of origin of individuals, and this information is not available, their nationality could be used as a proxy. However, this proxy does not seem to be accurate enough to determine the country of origin of certain individuals.[32] Representation error concerns the question of how representative the sample population is. If some groups of the general population are not sufficiently represented in the sample, the output could be incorrect and biased. The FRA also highlights the importance of timeliness of the training data; in other words, training data should represent individuals at the present time.[33]

In this respect, the question arises regarding which type of data should be included in the machine to avoid bias and hence discrimination (de-biasing data). The issue is that detecting and eluding discrimination is not straightforward. Indeed, it has been concluded that AI systems designed to be neutral can still produce discriminatory outcomes; that is to say, the risk will not be easily solved solely by removing the information directly referred to protected grounds (e.g., race, ethnicity, or gender). In fact, there might be some proxies or residual information which still refer to individuals' protected attributes.[34]

Završnik raises an interesting debate about whether it is desirable or not to conduct de-biasing procedures. He considers that this would not be suitable if choices about data are taken "behind closed doors by computer scientists in a laboratory".[35] Then he poses the question about whether our society would prefer human bias or machine bias. Although the latter discussion would be out of the scope of this paper, it is worth mentioning that the design of the AI system should involve not only computer experts, but also lawyers; and, in any case, the process should be transparent and not happen "behind closed doors". In the author's view, human overview and transparency throughout the whole process are key elements for preventing discrimination and biased outcomes. In this regard, the FRA highlighted the relevance of periodically auditing AI systems. Although there still is little research on which datasets provoke discriminatory predictions, there are already methods to detect which information contributes most to AI systems' outcomes.[36] This is the first step to improve AI systems' fairness.

As with the presence of biased data, AI systems' technical miscodes or errors can also be responsible for discriminatory outcomes. These errors should also be solved in the design process, since they could increase the unequal rates of 'false positives' and 'false negatives'. However, it should be remembered that this is not always due to wrong codes

(Florida State University), 2010.

[28] See M. Hamilton, *The Biased Algorithm: Evidence of Disparate Impact on Hispanics*, in *American Criminal Law Review*, vol. 56, 2019, 1553-1577; M. Hamilton, *The sexist algorithm*, in *Behavioral Sciences & the Law*, vol. 37, 2019, 145-147.

[29] See "*Dutch scandal serves as a warning for Europe over risks of using algorithms"* www.politico.eu /article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms accessed 17 April 2023.

[30] "*Poland: Government to scrap controversial unemployment scoring system"* https://algorithmwatch.org /en/poland-government-to-scrap-controversial-unemployment-scoring-system accessed 17 April 2023.

[31] In a similar vein, see A. Završnik, *Algorithmic justice: Algorithms and big data in criminal justice settings*, in *European Journal of Criminology*, vol. 18, 2019, 623-642.

[32] European Union Agency for Fundamental Rights, *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, 11.

[33] *Ibid*., 12.

[34] European Union Agency for Fundamental Rights, *#BigData: Discrimination in data-supported decision making,* 8.

[35] A. Završnik, *Algorithmic justice: Algorithms and big data in criminal justice settings*, 633.

[36] European Union Agency for Fundamental Rights, *#BigData: Discrimination in data-supported decision making*, 6.

programmed in the machine, since the presence of biased factors is still one of the main reasons of these disparate results.[37]

2.2.2. *Risk of AI systems' opacity*

As previously stated, it is possible to differentiate between explainable and interpretable AI models (e.g., decision trees) and deep-learning 'black-box' AI models (e.g., neural networks). Both pose a risk of discrimination, but 'black-box' models also carry a risk of opacity and a lack of explainability. They are known as 'black boxes' because the decision-making process remains opaque. This opacity may be due to three different reasons which were mentioned before, and which Burrell names as: intentional opacity, illiterate opacity, and intrinsic opacity.[38] Intentional opacity refers to algorithms that are protected by trade secrets or intellectual property rights (e.g., COMPAS).[39] Illiterate opacity arises when the tool is only understandable for computer scientists who can read machine codes. Finally, intrinsic opacity refers to AI systems which are uninterpretable to any human user. All combinations between these types of opacity are possible.

In all three cases, the lack of transparency and explainability jeopardises citizens´ right to data protection. For instance, individuals may not be able to challenge an administrative resolution if part of its reasoning is opaque (e.g., Polish unemployment profiling tool). Additionally, intrinsic opacity constitutes a barrier for designers and developers of the AI system. This is perhaps the most worrying form of opacity, since no person would be able to explain how a certain prediction was made. Hence, it will not be possible to detect potentially biased outcomes, nor will it be possible to initiate a de-biasing procedure.

Having said this, it is necessary to explain the difference between transparency and explainability in the context of AI systems. In this regard, a study conducted by the European Parliament Research Services is very enlightening.[40] According to it, transparency is the availability of the AI model's code, design documentation and learning dataset. However, it does not mean that it is available to the public. As for explainability, it is the availability of explanations about the logic behind the AI systems' decision.

Bearing in mind the latter, it seems that only a transparent AI system can properly address the risks posed to citizens' fundamental rights. Indeed, transparent, and explainable AI systems should be the final aim. For citizens' rights not to be hampered, there is a need for justifications to the reasoning made by the tool. A mathematical or technical explanation of how the algorithm evolved from the input to the output will not suffice.[41]

Therefore, the question is how to implement 'explainability'. The aforementioned European Parliament's study describes three possible approaches:[42] a black-box approach, a white-box approach and a constructive approach. The first one analyses the relationship between the inputs and outputs of the AI system without any knowledge of its code. The white-box approach considers that analysing the code is feasible. Lastly, the constructive approach operates by inserting explainability requirements in the design process of the tool.[43]

In this vein, there are already some techniques which address these approaches. For instance, so-called model-specific techniques, which incorporate interpretability within the structure of 'black-box' models; or model-agnostic techniques which use the inputs and predictions of the 'black box' to produce explanations (explainable AI (XAI)).[44]

[37] To see a graphic example on disparate results between two groups due to the presence of biased factors, see R. Courtland, *The bias detectives*, in *Nature*, vol. 558, 2018, 357-360.

[38] J. Burrel, *How the machine "thinks": Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 2015, 2.

[39] COMPAS originated the *Loomis v. Wisconsin* case, in which Loomis argued that using predictive algorithms violated his right to due process because they did not allow him to verify the scientific validity and accuracy of such algorithms. (See Taylor R. Moore, *Trade Secrets Algorithms as Barriers to Social Justice* in *Center for Democracy and Technology*, and Council of Bars and Law Societies of Europe, *Considerations on the legal aspects of artificial intelligence* (CCBE), 2020, 24.

[40] European Parliament Research Services (Panel for the Future of Science and Technology), *Understanding algorithmic decision-making: Opportunities and challenges*, 2019, 3.

[41] For the distinction between justification and explanation, see S. Quattrocolo, *An introduction to AI and criminal justice in Europe*, in *Revista Brasileira de Direito Processual Penal*, vol. 4, 2019, 1528.

[42] These approaches will be further elaborated in section 3.2 "transparency as a means to explainability".

[43] European Parliament Research Services (Panel for the Future of Science and Technology), *Understanding algorithmic decision-making: Opportunities and challenges*, 2019, 4.

[44] A. Rai, *Explainable AI: from black box to glass box*,

From the above, it can be concluded that the main risk with regard to the tool's opacity is the lack of explainability. In fact, although full transparency of the code and mechanism of the AI system is desirable, in order to exercise their rights, citizens may also need an explanation of the logic involved behind the AI system. However, in any case, it is quintessential that the system also be transparent. Indeed, transparency should be seen as a means to an end.[45] The end is having an explainable and unbiased AI system which respects fundamental rights like the right to privacy and data protection. Consequently, it is required that the entire algorithmic process be transparent so as to enable regulators, designers, auditors, deployers and developers, to detect and address its flaws. This is the first step to ensure the implementation of a fair AI system.

2.2.3 *Risk of falling into automation*

Algorithmic risk-assessment tools are part of ADMSs. Therefore, taking SyRi´s example, there will be an automation component in the decision-making process which may jeopardise decision makers' discretion. If this occurs, the right to privacy and data protection will be affected since the risk score issued by the tool can interfere in citizens´ private life. In this regard, these tools should be conceived as an additional element to aid decision makers in reaching a decision. In fact, the opposite would be in breach of Article 22 of the GDPR (right not to be subject to a decision based solely on automated processing, including profiling).

The European Commission strongly affirms that AI should follow a human-centric design approach.[46] This is especially important in the context of public services, where citizens should be put at the centre. As it was mentioned before, human overview throughout the whole process is a key element to address the different risks posed by this kind of tools. The "surveillance" during the design process by IT experts and data protection experts would act as a safeguard for citizens' fundamental rights. This would be a crucial element to detect possible biases or errors produced by the tool.

However, the question here is how to ensure that decision makers do not fully rely on the decision given by the tool. Indeed, human overview cannot mean a decision maker "just signing off the recommendations or outputs from an algorithm".[47] Ultimately, the problem lies in the so-called 'control problem', which states that humans tend "to fall into automation complacency and bias once the system operates reliably most of the time".[48]

In the case of the Polish AI system, the technology was initially projected as an advisory tool for public servants as decision makers of a case. However, it turned out that decision makers overrode less than 1 in 100 decisions.[49]

3. *EU Data Protection Framework: instruments to address the risks of algorithmic risk-assessment tools*

3.1. *Introduction*

The right to privacy and the right to personal-data protection are enshrined in Articles 8 of the ECHR and Articles 7 and 8 of the EU Charter of Fundamental Rights. They are closely related to each other since they both strive to protect individuals' autonomy and human dignity. However, they differ in their scope and formulation. The right to privacy –referred to in Articles 7 of the EU Charter and 8 of the ECHR as the right to respect for private and family life– is invoked whenever an interference in the individual's private sphere has occurred. By contrast, the right to personal-data protection is broader since it comes into play whenever personal data are being processed.[50] In this regard, risk-assessment tools are likely to process personal data, e.g., SyRi processed large amounts of personal data which included, *inter alia*, work

138.

[45] This idea was expressed by J. Cobbe at the 14th International Conference Computers*, Privacy & Data Protection: Enforcing Rights in a Changing World* (27-29 January 2021).

[46] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, Brussels, 2020, 3; and European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Brussels*, 2021, 1.

[47] *Mutatis mutandis*: European Union Agency for Fundamental Rights, *Getting the future right. Artificial Intelligence and Fundamental Rights*, Vienna, 2020, 64.

[48] J. Zerilli et al., *Algorithmic Decision-Making and the Control Problem*, in *Minds and Machines*, vol. 29, 2019, 565.

[49] Joint Research Centre (European Commission), *AI Watch. Artificial Intelligence in public services. Overview of the use and impact of AI in public services in the EU*, Brussels, 2020, 47.

[50] European Union Agency for Fundamental Rights, *Handbook on European data protection law*, Vienna, 2018, 19-20.

data, education data, personal identification data (e.g., name, address, city).[51] Consequently, this kind of AI tools would trigger the application of data protection rules and citizens would be considered as data subjects.

In this regard, the processing of personal data by these tools would require having a legal basis as per Article 6 of the GDPR. In the case of SyRi, there was a legal basis enshrined in Dutch law,[52] but this was certainly not sufficient to guarantee the right to privacy and data protection. In the following sections, different instruments offered by the existing Data Protection Framework will be analysed in light of the risks previously identified. This analysis will provide some guidance on how to address these challenges and on how to work towards the implementation of human-centric AI systems in the public sector.

3.2. *Transparency as a mean to explainability*

The principle of transparency is one of the core principles regulated by the GDPR in Article 5. This requirement is quintessential to the rights concerning the processing of people's personal data (e.g., right of access, right to rectification or erasure of personal data). Indeed, this requires the information shared with data subjects "to be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used" (Recital 58 of the GDPR).

Transparency addresses the risk of opacity, which hampers the right to data protection. In concrete, regarding SyRi, the Hague District Court, in February 2020, delivered a judgement where it decided that SyRi legislation did not comply with Article 8 of the ECHR mainly because of lack of transparency. The risk model and the risk indicators were 'secret' and the legislation provided no duty to inform data subjects that their data were being processed in SyRi.[53] Consequently, there is a need to make 'black-box' systems transparent. In this regard, transparency is a means to achieve the aim of explainable and unbiased AI systems pursued by citizens' fundamental rights.

There are already different methods and approaches to tackle the 'black-box' issue as already introduced in sub-section 2.2.2. The European Parliament Research Services distinguishes between three approaches to an explainable AI system. First, the black-box approach which demands to explain complex and difficult AI systems without any knowledge of the code, in other words: without "opening" the 'black box'. Second, the white-box approach makes it possible to analyse the code of the system by providing explanations to a wider range of AI systems (e.g., deep neural networks). Last, the constructive approach refers to situations where explainability is built during the design process of the AI system.[54]

Both the black-box and white-box approaches consist of explaining 'black-box' systems with separate explanation models. These models help to make those AI systems explainable. For instance, Local Interpretable Model-Agnostic Explanation (LIME) works by implementing an interpretable model to a specific outcome produced by an opaque system.[55] Conversely, the constructive approach aims to build an inherently interpretable model without requiring second models to explain the 'black box'. Thus, it consists of "originally" interpretable and transparent AI systems (see sub-section 2.2.2).

Having said that, the scientific community has drawn attention to the trade-off between explainability and accuracy. In this sense, a big part of the research community advocates for the reliance on the first two approaches. This scholarship considers that despite how easy it is to build intrinsically explainable models, the simpler these models are, the less accurate their results will be. Therefore, their proposal is to build complex but highly accurate 'black-box' models and then explain their inner functioning with second *post-hoc* models.[56] This entails that a certain degree of

[51] The Hague District Court, C/09/550982/HA ZA 18-388 Judgment of 5 February 2020 paragraph 4.17 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 accessed 17 April 2023.

[52] The Hague District Court, C/09/550982/HA ZA 18-388 Judgment of 5 February 2020 paragraph 4.8 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 accessed 17 April 2023.

[53] The Hague District Court, C/09/550982/HA ZA 18-388 Judgment of 5 February 2020 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 accessed 17 April 2023.

[54] European Parliament Research Services (Panel for the Future of Science and Technology), *Understanding algorithmic decision-making: Opportunities and challenges,* 2019, 48-52.

[55] Information Commissioner's Office and The Alan Turing Institute, *Explaining decisions made with AI*, 2020, 124.

[56] See Sarkar et al., *Accuracy and interpretability trade-offs in machine learning applied to safer gambling*, in CEUR Workshop Proceedings, vol. 1773, 2016; Z.C.

transparency and explainability be provided once the model has already been deployed. On the other hand, another part of the literature supports the constructive approach where transparency is provided in the design process before the implementation of the model.[57]

Rudin is of the opinion that, although challenging, it is possible to design interpretable models which provide their own explanations while also being accurate. Indeed, she clarifies that using second *post-hoc* models entails the risk that "any explanation method for a black-box model can be an inaccurate representation of the original model in parts of the feature space". [58]

In light of the above, opting for a constructive approach would be the best option to meet the requirements of transparency and explainability. If risk assessment tools are based on an interpretable model, data subjects, would be in a better position to understand how the tool reached the risk score as well as which attributes it took into consideration, and hence they will be able to know how their personal data are being processed. This is the type of information that was not provided to citizens being subject to the Polish unemployment tool. Individuals' inability to understand how the tool had reached the score made it difficult for them to later challenge the administrative decision. Indeed, Rudin affirms that it is easier to detect and avoid possible bias and data privacy issues within an interpretable model than within a 'black box'.[59] For this reason, it is necessary to invest in research and design processes of AI systems so to implement an explainable while accurate interpretable model. In this regard, this would be a decision of "data protection by design" where transparency could be effectively embedded into the tool (see section 3.3).

Nevertheless, this explainability strategy does not solve the issue with intentional 'black-box' systems where there is a trade secret or intellectual property right over the technology. Indeed, the model could be interpretable but still protected by intellectual property rights. In this regard, Recital 63 of the GDPR mentions that the right to access personal data "should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property". As the Norwegian Data Protection Authority (hereafter Norwegian DPA) suggests, a balanced solution could be achieved by providing data subjects with the information they need to protect their interests, while not disclosing trade secrets.[60] Therefore, the trade-off between IP rights and the requirements of transparency and explainability is an interesting angle to address in future research.

Having addressed how transparency and explainability can be technically achieved, it is useful to assess what the explainability requirement should include. In this regard, Wachter et al. distinguish between two kinds of explanations to be provided when an automated tool is involved. The first one refers to the system functionality which includes the general functionality of the automated decision-making system, the models, the logic, or the classification structures. The second one refers to the specific decisions, which are the rationales, reasons and individual circumstances that led to a concrete automated decision. The latter kind of explanation is the one referred to in Recital 71 of the GDPR ("…to obtain an explanation of the decision reached after such assessment and to challenge the decision"). Then, these authors differentiate between an explanation given *ex ante* and *ex post* automated decisions.[61] It should be noted that although Article 15 of the GDPR on the right of access does not mention a specific timing for the exercise of this right, the explanation should be given *ex ante* and *ex post* to the processing of the data by the tool.

According to Articles 13 (information to be provided where personal data are obtained

Lipton, The Mythos of Model Interpretability in Machine Learning, the concept of interpretability is both important and slippery, in *Association for Computing Machinery*, 2018; B. Lepri et al., *Ethical machines: The human-centric use of artificial intelligence*, in *iScience*, vol. 24, 2021.

[57] See R. Caruana et al., *Intelligible Models for HealthCare: Predicting Pneumonia Risk and Hospital 30-day Readmision*, in *KDD '15: Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, 1721-1730; B. Letham et al., *Interpretable classifiers using rules and Bayesian analysis: building a better stroke prediction model*, in *The Annals of Applied Statistics*, vol. 9, 2015, 1350-1371; C. Rudin, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, in *Nature Machine Intelligence*, vol. 1, 2019, 206-215.

[58] C. Rudin, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, 207.

[59] *Ibid*., 208.

[60] Datatilsynet (The Norwegian Data Protection Authority), *Artificial intelligence and Privacy*, 2019, 19.

[61] S. Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. 7, 2017, 78.

from the data subject), 14 (information to be provided where personal data have not been obtained from the data subject), and 15 (right of access) of the GDPR, the data subject has the right to be informed of the purposes and categories of personal data that are subject to the processing activity. The processing must be lawful, fair, and transparent, which entails that the data subjects should be aware of how their data are being processed. From this, it could be determined that the scope of the explanation should include both the system functionality and the specific decisions of the AI tool. In this vein, the Information Commissioner's Office (hereafter ICO) identifies different ways to explain AI decisions, which include a rational explanation, a data explanation, and a fairness explanation.

The rationale explanation refers to the reasons behind a certain decision so to allow individuals to challenge the decision in a proper form. These are the specific decisions of AI tools explained in an accessible and non-technical manner.[62] The data explanation should inform individuals not only about what data have been used and how, but also about what other types of data have been used to design, train and test the AI model.[63] This entails providing information on the quality of the data so to prove that data sets are free from bias and that the training data are periodically verified and tested. Therefore, this explanation encompasses the input data (personal data of the individual) and the training data (historical data). In this regard, the proposal for an AI act includes among the information to be provided to users: "specifications for the input data, or any other information in terms of the training, validation and testing data sets used".[64] Last but not least, the fairness explanation consists of fostering trust among individuals subject to automation by informing them about the steps taken to design and implement an AI model which is unbiased, fair, and non-discriminatory.[65]

In a sense, it can be said that the last two kinds of explanations defined by the ICO offer information on the system functionality. However, it should be mentioned that technical or mathematical explanations should be provided to the extent necessary to understand the logic of the tool and to determine how it finds correlations and patterns within the dataset. In fact, the Norwegian DPA opines that "it is not always necessary to provide a thorough explanation of the algorithm, or even include the algorithm".[66] Therefore, the author of this paper understands that the information on the system functionality should be provided in order to allow data subjects to readily understand how the decision was made without delving into unnecessary technical aspects. Consequently, such a transparent explanation would enable individuals to verify whether their data are being processed fairly and lawfully. If this is not the case, they could submit a data-protection request to the controller of their personal data or even lodge a data-protection complaint before the corresponding Data Protection Authority.

3.3. *Privacy and data protection by design or "AI systems by design"*

Article 25 of the GDPR establishes the obligation of the controller "to implement appropriate technical and organisational measures (…) which are designed to implement data protection principles". This entails that the controller (the public authority implementing the AI system) is required to have data protection designed into the processing of personal data. In this sense, unlinkability, transparency and control over the data constitute entry points and goals to privacy by design processes.[67]

Consequently, in the context of risk assessment tools, this provision mandates that transparency be implemented in the design process of AI technology. In this regard, as it has been analysed throughout this contribution, the choice of an explainable AI system should be made during the design process of the tool so to comply with this legal requirement. In other words, opting for a constructive approach where explainability is built during the design process of the AI system. Indeed, the AI act highlights the relevance of design choices of high-risk AI systems.[68] As Bryson indicates, the extent to which transparency is embedded into a

[62] Information Commissioner's Office and The Alan Turing Institute, *Explaining decisions made with AI*, 2020, 20 and 23.
[63] Ibid., 25-26.
[64] Article 13 Proposal for a Regulation of AI.
[65] Information Commissioner's Office and The Alan Turing Institute, *Explaining decisions made with AI,* 28-29.
[66] Datatilsynet (The Norwegian Data Protection Authority), *Artificial intelligence and Privacy*, 21.
[67] Spanish Data Protection Authority (AEPD), *A Guide to Privacy by Design*, 2019, 13 www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf accessed 17 April 2023.
[68] Article 10 Proposal for a Regulation of AI.

product constitutes a design decision and it is perfectly possible to achieve that the technology is designed to comply with laws.[69]

Having said the above, the design process of algorithmic risk-assessment tools is important to provide the tool with transparency and explainability, but it is also crucial to avoid other risks that would threaten citizens' fundamental rights. On the one hand, an adequate privacy by design strategy will ensure that personal data are stored in a secure manner and that data-protection principles be respected. On the other hand, a robust and careful design will also address the risk of biased outcomes by selecting the correct quantity and quality of the training data, or by developing a machine code that avoids undesired results. In this regard, the selection of an inherently interpretable model could already enable regulators, designers, auditors, deployers and developers, to detect and address its flaws before its implementation. To this should be added the importance of documenting the design decisions, not only to be able to provide a full explanation of how the tool reached a certain decision, but also to demonstrate compliance of the AI system with the requirements set out in the Proposal.[70] Moreover, this Proposal requires that these tools include record-keeping or logging capabilities that enable traceability of their functioning.[71] The latter requirements will facilitate audits and monitoring of the technology to correct possible errors or flaws.

In the field of data protection, it is considered that the design must be kept "user-centric" to guarantee the rights and freedoms of the users whose data are processed.[72] Similarly, the European Commission strongly affirms that AI should follow a human-centric design approach,[73] which centres individuals' needs, motivations, emotions, or behaviour in the development of the design.[74] As a consequence, and especially in the public sector, every design decision of the AI tool should be inspired by this approach with the aim to preserve citizens' fundamental rights ('citizen-centric approach'). Therefore, the author considers that the decision to opt for an inherently explainable AI system places humans in the centre. In any case, it would be advisable to adopt a participatory design[75] where computer scientists, engineers and mathematicians work closely with bar associations, lawyers, data-protection experts, or civil-society organisations in the design of the prospective algorithmic risk-assessment tool. Moreover, citizens' perspective should also be taken into consideration. This can be achieved through the establishment of an AI register (see also 3.5), conducting public campaigns informing about the initiation of an AI system project, collecting feedback from citizens on the prospective objectives and design of the tool… In this way end-users would be involved in the design process of the technology and their interests could be reflected in the final architecture of the tool. This will also help public authorities decide on whether it is feasible or not to proceed with the different phases of a concrete project.

These design options and decisions can be tested through regulatory sandboxes. The latter constitutes an interesting mechanism introduced by the Proposal for an AI act where public authorities as regulators together with innovators can test AI systems in a safe environment before placing them on the market or putting them into service. The first regulatory sandbox on AI was presented on June 2022 by the government of Spain and the European Commission. National authorities from other Member States should also be encouraged to do so.[76]

[69] J. Bryson, *The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation*, in M.D. Dubber et al (ed.), *The Oxford Handbook of Ethics of AI*, in Oxford Handbooks Online, 2020, 5.

[70] Article 11 Proposal for a Regulation of AI.

[71] Article 12 Proposal for a Regulation of AI.

[72] Spanish Data Protection Authority (AEPD), *A Guide to Privacy by Design*, 2019, 10 www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf accessed 17 April 2023.

[73] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, 2020, 3; and, European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, Brussels, 2021, 1.

[74] See B. Shneiderman, *Human-Centered Artificial Intelligence: Three Fresh Ideas*, in *AIS Transactions on Human-Computer Interaction*, 2020.

[75] J. Auernhammer, *Human-centered AI: The role of Human-centered Design Research in the development of AI,* in *Synergy - DRS International Conference*, 2020, 1320-1321.

[76] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, Brussels, 2021, Recital 71 and 72; 'First regulatory sandbox on Artificial Intelligence presented' https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented accessed 17 April 2023.

3.4. *Data Protection Impact Assessment and Algorithmic Impact Assessment*

Data Protection Impact Assessments (hereafter DPIAs) constitute a requirement to be fulfilled by data controllers when the processing of personal data using new technologies is likely to result in high risks to the rights and freedoms of individuals. DPIAs should include the envisaged measures and safeguards to address the risks to rights and freedoms of data subjects (Article 35 of the GDPR). In this regard, the implementation of an AI risk-assessment tool in the public sector would be considered as a new technology that would process personal data and pose high risks to citizens' fundamental rights. Hence, DPIAs should be conducted before implementation to identify the risks of the tool, to reflect on how to tackle them, and to select appropriate mitigating measures to those risks. Therefore, a similar exercise to the one conducted in this paper.

In the case of SyRi, the Court concluded that the only existing DPIA was delivered before the GDPR entered into force and that such assessment was not done for each of the five projects carried out under SyRi legislation.[77] Moreover, it is clear that the principle of transparency towards individuals was not properly addressed in that DPIA since the Court considered that this principle was "insufficiently observed in the SyRi legislation" and that "in no way provides information on the factual data that can demonstrate the presence of a certain circumstance, in other words which objective factual data can justifiably lead to the conclusion that there is an increased risk".[78]

Similarly, in the field of AI, Algorithmic Impact Assessments (hereafter AIAs) are deemed necessary to evaluate the potential impact of algorithmic systems before their deployment. In this regard the European Parliament Research Services opines that ADMSs should not be implemented without a prior AIA except when it is certain that they will not have a significant impact on individuals' lives.[79] The AINow Institute elaborated a report on AIAs where it stressed that the benefits of conducting such an assessment can help identify the "potential issues of inaccuracy, bias and harms to affected communities" and determine possible ways to address these impacts while involving affected community members in that process.[80] In this regard, the Government of Canada has released a Directive on Automated Decision Making which requires the completion of an AIA prior to the production of any ADMSs. In concrete, an AIA risk-assessment tool has been developed to score the impact level of ADMSs. [81]

At the EU level, the proposal for an AI act includes the obligation to conduct a "conformity assessment" to demonstrate compliance with the requirements for high-risk AI systems (e.g., transparency, record-keeping), but there is no reference to an instrument like the AIAs.[82] Although conducting conformity assessments is a frequent scheme for the placement of products in the market in the EU, the author considers that in the case of AI systems this would not suffice, especially because this is a one-time assessment. Apart from carrying out a DPIA, it would be necessary to conduct an AIA which is made publicly available to increase transparency and explainability, and to allow citizens to exercise their rights.[83] This should be included in the public database proposed in the AI act in order to show the risks of the AI system and the measures taken to address them. Indeed, this is also remarked by the EDPB and the EDPS in their Joint Opinion: "this database should be taken as an opportunity to provide information for the public at large on the scope of application of AI system and on known flaws and incidents that might compromise their functioning and

[77] The Hague District Court, C/09/550982/HA ZA 18-388 Judgment of 5 February 2020 paragraphs 6.103-6.105 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 accessed 17 April 2023.

[78] The Hague District Court, C/09/550982/HA ZA 18-388 Judgment of 5 February 2020 paragraph 6.87 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 accessed 17 April 2023.

[79] European Parliament Research Services (Panel for the Future of Science and Technology), *Understanding algorithmic decision-making: Opportunities and challenges*, 2019, 88.

[80] D. Reisman et al., *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*, in *AI NOW Institute*, 2018, 9.

[81] Canada's Directive on Automated Decision-Making: www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592 accessed 30 April 2021. Canada's AIA risk assessment tool: www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html accessed 17 April 2023.

[82] Articles 3(20) and 43 Proposal for a Regulation of AI.

[83] In this same regard, *see* Algorithmwatch, 'Civil society open letter demands to ensure fundamental rights protections in the Council position on the AI Act https://algorithmwatch.org/en/fundamental-rights-protections-in-the-council-position-on-the-ai-act/ accessed 17 April 2023.

the remedies adopted by providers to address and fix them".[84]

It is worth noting that, *in casu*, both DPIAs and AIAs would be helpful instruments to enforce compliance with transparency, explainability or unbiased requirements. However, the AINow Institute draws a distinction between them. First, while DPIAs are not shared with the public and apply to public and private organisations, AIAs are designed to engage with affected individuals, researchers, and policymakers. [85] In this regard, it seems that AIAs offer a broader scope for action than DPIAs since they may allow the participation of the ultimate users of the technology in the participatory design of the tool (see sub-section 3.3). In any case, this does not mean that DPIAs should not be conducted (indeed, they still constitute a legal obligation under Data Protection legislation), but in the field of AI, AIAs would complement DPIAs.

3.5. *Audits*

Audits are conducted in the field of data protection to assess a specific organisation's compliance with data protection legislation and to verify that appropriate safeguards are in place when personal data are being processed. Audits are included among the tasks of data-protection officers and supervisory authorities to monitor compliance with the provisions of the GDPR (Articles 39 and 57 of the GDPR). As the ICO indicates, audits are intended to be educative and not punitive. Their objective is to identify weaknesses, risks, or deficiencies in the processing practices in order to encourage compliance with data protection legislation.[86] In this vein, they would constitute a useful instrument to assess whether data protection and privacy by design choices are still valid once risk-assessment tools are implemented in the public sector. Moreover, an audit could focus on assessing AI systems for bias. In fact, in some Member States, like the Netherlands, AI systems used by government agencies have already been audited and assessed on their performance.[87]

In this regard, the EDPB and the EDPS, in their Joint Opinion on the AI Act, consider that high-risk AI systems shall be audited by a third party before obtaining the CE marking that would allow providers to place the product in the market.[88] In fact, it would be highly recommended that the results of periodic audits be registered in the public database included in the proposal for an AI act. According to Articles 51 and 60 of the Proposal, this register would contain information on the algorithmic tool e.g., description of the intended purpose of the AI system, contact details of the provider or a copy of the declaration of conformity assessment.[89] This would facilitate auditing tasks, but it would also enhance transparency. In this regard, as already indicated, for the sake of transparency, it would be advisable that an explanation of the model (logic involved behind it) as well as the results of any AIA and DPIA, be also included in the register.[90] The latter is lacking in the AI act.

In light of the above, a register that contains meaningful information on the AI system appears to be a right approach towards the aim of transparency and even explainability. If the register already includes information on the deployed model and the logic behind its reasoning, citizens could get acquainted with the system before being subject to it. Moreover, this register would allow stakeholders (e.g., lawyers, bar associations, data protection professionals) to provide feedback on the tools' design and hence contribute to build human-centric AI risk-assessment tools.[91]

4. *Conclusions*

The use of AI is on the rise in different

[84] EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 2021, 20.
[85] D. Reisman et al., *Algorithmic Impact Assessments*, 7.
[86] Information Commissioner's Office, *A guide to ICO audits*, 2018, 11.
[87] An audit of 9 algorithms used by the Dutch Government, https://english.rekenkamer.nl/publications/reports/2022/05/18/an-audit-of-9-algorithms-used-by-the-dutch-government accessed 17 April 2023.
[88] EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 10-11.
[89] Article 51 Proposal for a Regulation of AI and Annex VIII Proposal for a Regulation of AI.
[90] AlgorithmWatch, *Automating Society Report*, 2020 https://automatingsociety.algorithmwatch.org, 11; F. Reinhold and A. Müller, *AlgorithmWatch's response to the European Commission's proposal regulation on Artificial Intelligence – A major step with major gaps*, 2021 https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021 accessed 17 April 2023.
[91] The city of Amsterdam is currently developing an Algorithm Register where citizens will be able to provide feedback and hence participate in building human-centric algorithms in Amsterdam (City of Amsterdam Algorithm Register Beta https://algoritmeregister.amsterdam.nl/en/ai-register accessed 17 April 2023).

sectors and industries of society, including the public sector. This is evidenced by the recent legislative proposals issued by the European Commission in the context of AI, but also by the examples of AI systems and AI projects already tested in the public sector (e.g., SyRi or the Polish unemployment tool). These proposals show the efforts undertaken at EU level to ensure an adequate balance between stakeholders´ economic, commercial, or societal interests, and individuals´ fundamental rights. The implementation of these technologies can be beneficial for our society, but they threaten citizens' fundamental rights like the right to non-discrimination or the right to privacy and data protection. The latter has been the focus of this paper due to the vast amount of personal data usually processed by these AI systems. Therefore, this has triggered an analysis of the risks presented by AI systems and how they can be mitigated by looking at the current EU Data Protection framework. From this, it has been possible to extract some lessons on how to implement this technology by public administrations.

This contribution has identified three main risks regarding the use of AI systems: risk of discrimination, risk of AI systems' opacity, and risk of falling into automation. As it has been observed, the principles of transparency and explainability allow to address the risk of opacity and the risk of biased outcomes. In this regard, the data protection framework currently offers a variety of instruments and principles which strengthen the position of data subjects when confronting those risks: transparency, data protection by design, DPIAs and audits. However, throughout this paper, it has been noticed that the existing legislation requires to bear some considerations in mind in light of AI.

Firstly, to address the 'black-box' issue, a constructive approach where an inherently interpretable model is built would be recommended. This way the AI model would be transparent, and it would be possible to provide an *ex-ante* and *ex post* explanation of the process carried out by the tool. This explanation should include information on the specific decision reached by the tool (e.g., reasons behind the decision) and on the system functionality (e.g., quality of the data, design choices). Secondly, data protection by design mandates that transparency be embedded into the tool during its design process. To this aim, a human-centric AI approach where stakeholders and citizens participate in the design of the technology would be suitable to enhance transparency. Equally, citizens should be informed about the results of DPIAs and AIAs. All design choices and the results of the impact assessments should be documented and included in a publicly accessible register where citizens could provide feedback. These considerations are not fully covered by the proposed AI act.

In light of the above, the study conducted in this article has served to define some general requirements and considerations which can be taken into consideration when implementing a decision-making AI system in the public sector, but which can also be applicable to other sectors and domains. Indeed, the use of AI can directly or indirectly cause a significant impact on individuals' fundamental rights (this is the case of Dutch citizens' who were subject to SyRi's risk assessment). Therefore, it is required that those AI systems be transparent and explainable. In this regard, the AI act has proposed important measures in this field, but adequate requirements of transparency and explainability towards individuals are still lacking. In the author's view, there is still work to do to achieve the aim of a true human-centric AI.

With regard to the above, the AI act envisages the creation of an EU database where high-risk AI systems will be registered. However, the information to be contained in that register would be insufficient to achieve explainability. In addition to the certificate of conformity assessment, the register should contain the results of AIAs and DPIAs and meaningful information on the logic behind the tool. This will show the public what risks were identified and what measures were taken to prevent them. Moreover, this could engage citizens and relevant stakeholders in the process of designing or improving the AI system (participatory design). Indeed, a conformity assessment is not sufficient because although it would show that users and producers of AI products are compliant, it would not provide individuals with meaningful information on the functioning of the tool. These design options and choices can be tested through the establishment of regulatory sandboxes by public authorities which offer a safe environment to experiment with this technology before putting it into service.

To conclude, this research demonstrates that for the implementation of human-centric AI systems respectful with fundamental rights in

the public sector, it is necessary to ensure transparency during the whole process of designing, building and deployment of the technology. Transparency enables explainability, and explainability allows citizens to exercise their rights. This is why the organisation of public campaigns, conferences or participatory sessions with relevant stakeholders and citizens at the initial phases of an AI project can be helpful to build citizen-centric AI. Moreover, a human-centric AI approach requires continuous human oversight and especially in the public sector, it requires that humans are not replaced by machines, nor that they fall into automation. It remains to be seen how the final AI act will look like, but some remarks have already been included in this contribution. Some guidance can be found in the existing EU Data Protection framework.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 133-144
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 10

*L'identification en ligne du citoyen : la reconquête de son pouvoir de certification de l'identité par l'État**

Jessica Eynard
(Associate Professor, University of Toulouse Capitole-Private Law Institute (EA 1920))

ABSTRACT If the State has control over the identification of individuals in the real world, it has yet to conquer this faculty online at a time when the major platforms have developed their own identification tools. Several devices are thus emerging, in which the State plays an active role, directly or indirectly. On the whole, these systems deserve to be encouraged, although particular vigilance is required, at the risk of seeing identity become an ordinary object of the market, through the certification function.

1. *Introduction*

« Aujourd'hui plus que jamais, surtout depuis l'émergence de l'internet ; nous sommes identifiés chaque jour par les forces occultes du marché ; bien plus que par le pouvoir d'État »[1].

Genèse de l'identification[2] - L'histoire prouve que les acteurs de la société civile ont été les premiers à développer des moyens d'identification. D'abord fondée sur des pratiques traditionnelles d'interconnaissance, l'identification s'est peu à peu « professionnalisée » par l'établissement de listes, de tableaux et de registres. A l'origine, la connaissance de ses citoyens par le pouvoir nécessitait l'intervention d'intermédiaires locaux tels que des curés ou des notables. L'ordonnance du 15 août 1539 de François Ier exigeait en ce sens des curés qu'ils procèdent à l'enregistrement des naissances, des mariages et des décès. Petit à petit, l'État a commencé à jouer un rôle croissant dans l'identification des individus. L'adoption du décret du 20 septembre 1792 a abouti à confier aux maires, et donc à des représentants de l'État, le soin d'enregistrer l'état civil de l'ensemble des citoyens. Très rapidement, un écart s'est creusé entre l'identité réelle des personnes et leur identité légale et des solutions ont dû être trouvées pour pallier les déficiences de l'état civil. C'est ainsi qu'un système d'identification anthropométrique a été élaboré par Alphonse Bertillon. Cette même déficience de l'état civil explique aujourd'hui le recours à des identifiants biométriques, notamment dans des pays africains ou encore en Inde, où la fiabilité des registres peut être remise en cause.

L'histoire montre que, si l'État n'a pas été au fondement de l'identification, il s'en est saisi jusqu'à jouer un rôle fondamental tout au long du processus d'identification, que ce soit au moment de l'établissement de l'identité ou à celui de l'apport de la preuve de cette identité. Il n'est pas certain qu'il soit parvenu à tenir ce rôle dans le monde en ligne.

L'État, présent au moment de l'établissement de l'identité - A sa naissance, la personne doit être individualisée. Cela se fait par l'attribution d'une identité au nouveau-né lors de la déclaration de naissance à l'officier de l'état civil. Cette identité renvoie à « ce qui fait qu'une personne est elle-même et non une autre » et, par extension, à « ce qui permet de la reconnaître et de la distinguer des autres »[3]. Elle n'est pas définie par la loi française. Classiquement, elle renvoie à l'« ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalité, filiation, …) »[4]. Si elle individualise, l'identité ne confère pas un statut juridique à la personne, qui est acquis par l'établissement d'actes de l'état civil par un agent public, l'officier d'état civil[5], sous la responsabilité de l'État et le

* Article submitted to double blind peer review.

[1] G. Noiriel (éd.), *L'identification. Genèse d'un travail d'État*, Paris, Belin, 2007, 3.

[2] Sur cette partie, voir G. Noiriel (éd.), *L'identification. Genèse d'un travail d'État.*

[3] G. Cornu, *Vocabulaire juridique*, Association H. Capitant, Paris, PUF, 2020.

[4] *Lexique des termes juridiques*, Paris, Dalloz, 2014-2015.

[5] M. Bruggeman, *État civil et identité : quel(s) rapport(s) ?*, in J. Eynard, *L'identité numérique. Quelle définition pour quelle protection ?*, Bruxelles, Larcier, 2020.

contrôle du Procureur de la République. L'établissement de ces actes est entouré d'un formalisme important (mentions obligatoires, absence d'abréviation ou de date en chiffres, lecture des actes par l'officier qui invite les parties et témoins éventuels à en prendre connaissance[6]) qui s'explique par le fait que ces actes doivent parfaitement refléter la situation réelle de l'individu au moment où ils sont dressés mais également au gré des évolutions affectant l'état de l'individu[7], ce qui se manifeste par des ajouts en bas de page, en marge ou au verso de l'acte[8]. Pour davantage de sécurité, les actes de l'état civil sont soumis au principe de la reliure (pour éviter les fraudes et les pertes) et la tenue du double original. Il résulte de ces précautions que les actes de l'état civil sont considérés comme fiables. Ce faisant, ils sont utilisés pour l'établissement des moyens qui permettront à la personne de s'identifier.

L'État, présent au moment d'apporter la preuve de l'identité – Si l'identité peut se prouver par tous moyens, certains documents sont tout de même privilégiés. Le Conseil d'État observe en ce sens que, « si le principe de liberté de la preuve de l'identité d'une personne est consacré par la tradition républicaine, la création de la carte d'identité en 1955, puis le regroupement des fichiers des cartes d'identité et des passeports dans un fichier unique (le Fichier national de gestion) attestent la prééminence très forte acquise par les documents officiels – étatiques – d'identité dans cette certification »[9]. Les documents dont il s'agit reposent sur l'identité inscrite à l'état civil. Leur obtention nécessite qu'un acte de naissance soit fourni et qu'une vérification de la correspondance entre le document produit et la personne présente soit faite. Cette phase, appelée enrôlement, est particulièrement importante pour s'assurer de la correspondance entre l'identité demandée et l'identité réelle. Par la suite, la personne pourra produire sa carte d'identité ou son passeport pour prouver son identité, sans que la présentation de ces moyens ne devienne systématique[10]. Ce processus met en lumière le rôle joué par l'État puisque ce sont les moyens de preuve de l'identité qu'il produit qui sont utilisés en pratique, que ce soit par le secteur public ou le secteur privé. L'État se présente ainsi comme le garant de l'identité des usagers. Cette tâche semble néanmoins se dérober sous ses pieds lorsque l'identification a lieu en ligne.

L'État, absent an matière d'identification en ligne ? - Le réseau internet n'a pas été conçu pour permettre de déterminer qui est derrière la machine. L'identification concerne la machine elle-même et pas l'utilisateur. Pourtant, avec le développement de l'activité en ligne, le besoin de savoir avec un certain degré de certitude qui est connecté ou qui accède à tel ou tel service est devenu prégnant. Sont alors apparus les identifiants et les mots de passe. La multiplication des comptes, associés à chaque nouveau service a eu un effet pervers. Ces codes d'accès ont pu être oubliés, entraînant l'adoption de mots de passe identiques pour plusieurs sites et peu sécurisés (du type 1234). Certains acteurs ont en outre développé leur propre service d'identification de façon à devenir des intermédiaires permettant à l'internaute de s'identifier auprès d'un éventail de sites.

Cela amène à deux constats : « d'une part, l'utilité directe (des documents officiels) pour certifier son identité lorsqu'elle est demandée par un site internet est toute relative, pour ne pas dire inexistante ; d'autre part, surtout, la fonction de certification de l'identité est aujourd'hui très largement exercée par des plateformes numériques – Facebook à titre principal et Google également – sans intervention aucune de l'État »[11]. Le Conseil

[6] Voir pour les détails : Instruction générale du 29 mars 2002 relative à l'état civil.

[7] M. Bruggeman, *Le contenu de l'acte de naissance*, in C. Neirinck (dir.), *L'État civil dans tous ses états*, Paris, LGDJ, Series Droit et Société. Série Droit, 2008,

[8] Art. 49 du Code civil.

[9] Conseil d'État, *Étude annuelle 2017 Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, Paris, La documentation Française, spécialement 94.

[10] En effet, le principe de proportionnalité doit être appliqué de façon à ce que le moyen d'identification utilisé soit adapté au besoin de sécurité pour accéder au service. La Commission nationale de l'informatique et des libertés (CNIL) précise par exemple que la justification de l'identité « peut intervenir "par tout moyen". Ainsi, il n'est pas nécessaire de joindre une photocopie d'un titre d'identité en cas d'exercice d'un droit dès lors que l'identité de la personne est suffisamment établie (par exemple, par la fourniture d'informations supplémentaires à celles relatives à l'identité, comme un numéro client ou adhérent, etc.) ». Pour cette autorité de contrôle, « le niveau des vérifications à effectuer peut varier en fonction de la nature de la demande, de la sensibilité des informations communiquées et du contexte dans lequel la demande est faite », www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces.

[11] Conseil d'État, *Étude annuelle 2017 Puissance publique et plateformes numériques : accompagner l'«*

d'État parle ici d'« ubérisation » de la fonction de certification de l'identité. L'utilisation des boutons « Se connecter avec Facebook » et « Se connecter avec Google » sont en effet aujourd'hui largement répandus, ce qui participe à la collecte informationnelle sans fin opérée par ces acteurs et, par corrélation, à la remise en cause de droits et libertés fondamentaux. Pourtant, l'importance de pouvoir justifier d'une identité de façon fiable, et donc d'une identité reposant sur des éléments vérifiés et pas seulement déclarés, apparaît clairement quand il s'agit d'accéder à certains services.

Les enjeux de l'identification en ligne – Selon la Fédération de e-commerce et vente à distance, 2,3 milliards de transactions ont été réalisées sur des sites de vente sur internet en 2022, soit une hausse de 6,5% par rapport à l'année précédente[12]. La dématérialisation s'est aussi opérée en dehors du champ commercial, avec une intensification de la réalisation en ligne d'actes de la vie courante. La pandémie a aidé ce mouvement et on a vu par exemple apparaître la possibilité de se faire ausculter par un médecin et d'avoir un diagnostic en ligne. Tous ces actes impliquent de pouvoir identifier son co-contractant. En parallèle, les risques en termes de cybersécurité ont cru. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) considère que la menace cyber « se maintient à un niveau élevé », avec 831 intrusions avérées en 2022. Parmi les risques relevés, l'usurpation d'identité comprise largement comme l'utilisation d'une ou de plusieurs données relatives à une personne par une autre personne qui se fait passer pour elle afin d'obtenir un avantage, se trouve en bonne position. Dans son rapport sur l'usurpation d'identité, l'Agence européenne de la cybersécurité (ENISA) rapporte ainsi que 900 cas internationaux d'usurpation d'identité ou de délits liés à l'identité ont été détectés en 2019[13]. Ce chiffre n'est que la partie émergée de l'iceberg et on peut s'attendre à ce que les nombreuses violations de données, dont certaines sont régulièrement reprises dans les médias, se soldent par des usurpations d'identité à court, moyen ou long terme. Les possibilités d'usurpation permises par l'intelligence artificielle amplifient le phénomène, au moment où l'on s'inquiète du phénomène des « deepfakes ». Ces hypertrucages qui consistent à reproduire une voix ou à modifier un contenu visuel, tout en donnant l'impression d'une piste audio ou vidéo authentique, sont en pleine expansion. D'après les chercheurs de la société Deeptrace, le nombre de ces contenus truqués et volontairement trompeurs trouvés en ligne en 2019 étaient d'environ 15000, contre un peu moins de 8000 vidéos recensées un an auparavant[14]. Les conséquences pour les victimes de ces trucages, et les victimes d'usurpation d'identité plus largement, ne doivent pas être minimisées. Outre le préjudice économique qui peut en résulter, ces personnes se retrouvent souvent dans une situation complexe, leur imposant d'apporter une double preuve : celle de leur identité et celle de leur absence de culpabilité face à une infraction commise sur la base des informations dérobées. Ici, c'est le fait de pouvoir s'identifier avec certitude qui se présente comme essentiel.

Plan - L'État a indubitablement un rôle à jouer. Ce rôle s'inscrit en particulier dans les politiques européennes enjoignant les États membres à créer des schémas d'identification électronique[15] et à établir une identité numérique pour leurs citoyens[16]. L'objectif visé est de permettre à 80 % des citoyens de l'Union européenne d'utiliser une solution d'identification numérique pour accéder à des services publics essentiels d'ici à 2030[17]. Dans certains cas, l'État peut se révéler être le fournisseur du moyen d'identification en ligne. Dans d'autres cas, il recourt aux services d'opérateurs privés. En cela, il est tantôt un acteur direct (1), tantôt un acteur indirect (2) en matière d'identification en ligne.

ubérisation », 94.

[12] www.fevad.com/bilan-du-e-commerce-en-france-les-francais-ont-depense-pres-de-147-milliards-deuros-sur-internet-en-2022.

[13] ENISA, *L'usurpation d'identité. De janvier 2019 à avril 2020. Paysage des menaces de l'ENISA*, 2020, 2.

[14] www.oracle.com/fr/security/definition-deepfake-risques.html.

[15] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit règlement eIDAS, JOUE, L 257 du 28 août 2014, 74-114.

[16] Proposition de règlement européen modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021, COM(2021) 281 final.

[17] *Ibid*., 2.

2. *L'État, acteur direct en matière d'identification en ligne*

Le règlement eIDAS, adopté en 2014, a confié à chaque État membre le soin d'adopter un ou des schémas(s) d'identification électronique. Ce dernier est un « système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales »[18]. Le moyen d'identification électronique est lui-même défini comme « un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne »[19]. Concrètement, chaque État membre était invité à établir un processus d'identification, permettant la délivrance d'outils, grâce auxquels l'usager pouvait s'identifier en ligne, auprès de services proposés dans l'ensemble de l'Union européenne. Au moment de la publication de la proposition de règlement visant à modifier le règlement eIDAS et à établir un cadre européen relatif à une identité numérique[20], la Commission européenne relevait que seuls 14 États membres avaient notifié au moins un schéma d'identification électronique, de sorte que 59 % des résidents de l'Union européenne avaient en réalité accès à des schémas d'identification électronique fiables et sécurisés par-delà les frontières[21]. La France accuse un certain retard, en ayant notifié un seul schéma, permettant d'atteindre seulement un niveau de garantie substantiel qui plus est[22]. A l'échelon national, plusieurs outils assurant un niveau de garantie élevé ont pourtant été développés, mais sans faire l'objet d'une notification à la Commission européenne. Ainsi en est-il de l'application Alicem qui a été abandonnée avant sa diffusion auprès du public (1.1), et du Service de garantie de l'identité numérique (SGIN) qui vient à peine d'être lancé (1.2).

2.1. *L'échec d'Alicem*

L'application d'« Authentification en ligne certifiée sur mobile » connue sous le nom de Alicem est née avec le décret n° 2019-452 du 13 mai 2019[23]. Ce moyen d'identification électronique devait permettre aux usagers « de s'identifier électroniquement et de s'authentifier auprès d'organismes publics ou privés, au moyen d'un équipement terminal de communications électroniques doté d'un dispositif permettant la lecture sans contact du composant électronique de ces titres, en respectant les dispositions prévues par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 susvisé, notamment les exigences relatives au niveau de garantie requis par le téléservice concerné »[24]. Dit simplement, l'outil Alicem avait été conçu pour permettre aux usagers de s'identifier et de s'authentifier en ligne à l'aide d'un téléphone portable capable de lire la puce électronique présente sur le passeport ou le titre de séjour de l'utilisateur, grâce à une technologie sans contact. Ces modalités ne posaient aucune difficulté. Elles ne permettaient néanmoins pas d'atteindre un niveau de garantie élevé, lequel requiert de respecter des spécifications techniques, des normes et des procédures propres à empêcher l'utilisation abusive ou l'altération de l'identité[25]. Une couche supplémentaire de sécurité avait donc été prévue. L'utilisation de Alicem exigeait au surplus le respect d'un processus de vérification de l'identité incluant un système de reconnaissance faciale dynamique et statique. L'application proposait ainsi des défis à la personne qui devait en valider trois. L'utilisateur se voyait par exemple proposer de cligner des yeux, de tourner la tête à droite, puis à gauche ou encore de sourire. Le but était de s'assurer que l'application était utilisée par une personne vivante et non sa représentation sur une photo ou son cadavre. Puis, une comparaison était faite entre une photographie extraite de la vidéo faite au moment des défis et la photographie présente sur le passeport ou le titre de séjour. Il s'agissait alors d'authentifier

[18] Art. 3, paragraphe 4, du règlement eIDAS.
[19] Art. 3, paragraphe 2 du règlement eIDAS.
[20] Depuis cette date, de nouveaux schémas d'identification électronique ont été notifiés. Il est possible d'en prendre connaissance à l'adresse https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.
[21] Proposition de règlement modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, Exposé des motifs, 2.
[22] Le règlement eIDAS établit une échelle avec trois niveaux de garantie, à savoir les niveaux faible, substantiel et élevé.
[23] Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », JORF n° 0113 du 16 mai 2019.
[24] Art. 1er du décret n° 2019-452 du 13 mai 2019, *op.cit*.
[25] Art. 8, paragraphe 2, point c) du règlement eIDAS.

la personne grâce à une caractéristique biométrique. Alicem et en particulier le recours à la reconnaissance faciale ont fait l'objet de nombreuses critiques. Au-delà de l'émotion qu'il a suscité dans l'opinion publique[26], des arguments juridiques remettant en cause la légalité de ce dispositif ont été soulevés.

En particulier, la base juridique retenue pour fonder le traitement de données personnelles sous-jacent à l'identification a été questionnée. Classiquement, le consentement ne constitue une base juridique appropriée au sens de l'article 6 du RGPD que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées et si, dans ce dernier cas, elle ne subit aucun préjudice du fait de son refus[27]. Pour cette raison, le consentement ne peut être présumé avoir été donné librement dans certaines situations. Tel est le cas du consentement donné par un salarié pour un traitement mis en œuvre par son employeur ou du consentement donné par un administré à un traitement géré par une autorité publique quand les circonstances rendent improbables le recueil d'un consentement libre[28]. Comme il prenait appui sur le consentement, la validité du dispositif Alicem a pu donc légitimement être interrogée[29]. En réalité, le consentement était utilisé à double titre : d'une part, en tant que base de licéité du traitement et d'autre part, en tant qu'exception à l'interdiction de traiter des données sensibles[30]. Dans les deux cas, le recours au consentement peut faire l'objet de réserves[31]. Concernant tout d'abord la base légale du traitement, la base naturelle en matière de traitement public, à savoir la nécessité du traitement pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable, aurait dû être préférée. Dans le même sens, le choix du consentement pour justifier le traitement de données sensibles paraît étonnant quand, parmi les exceptions permettant de déroger à l'interdiction d'un tel traitement, on trouve la nécessité du traitement pour un motif d'intérêt public important. Le Comité consultatif de la Convention 108 considère en outre que « le consentement ne devrait pas être le fondement juridique utilisé pour la reconnaissance faciale effectuée par les autorités publiques compte tenu du déséquilibre des pouvoirs entre les personnes concernées et ces autorités »[32]. Le choix du consentement dans ces cadres, a certainement été motivé par le fait qu'il apparaît moins contraignant à mettre en œuvre que les fondements classiques. Il évite en effet de devoir justifier de la nécessité du traitement pour un motif d'intérêt public important (dérogation pour traiter des données sensibles) ou de sa nécessité pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable (base légale du traitement). En ce sens, la question de la légitimité du consentement comme fondement au traitement de données en vue d'identification reste en suspens.

Le Conseil d'État, saisi du point de savoir si le dispositif Alicem était légal, n'a pas répondu à cette question. Dans un arrêt du 4 novembre 2020[33], il s'est interrogé sur la liberté du consentement, en faisant complètement abstraction de la question de la légitimité du consentement qui aurait dû être préalable. Il décide de valider le moyen d'identification Alicem en considérant que la liberté du consentement est préservée dans la mesure où l'usager peut accéder à l'ensemble

[26] Parmi les nombreux articles de journaux, il est possible de se reporter à www.laquadrature.net/2019/07/17/la-quadrature-du-net-attaque-lapplication-alicem-contre-la-generalisation-de-la-reconnaissance-faciale ; www.numerama.com/politique/559511-alicem-tout-comprendre-au-dispositif-de-reconnaissance-faciale-controverse-du-gouvernement.html ; www.lesnumeriques.com/vie-du-net/alicem-pourquoi-le-systeme-de-reconnaissance-faciale-de-l-etat-suscite-la-controverse-a142589.html ; https://actu.fr/societe/alicem-pourquoi-lapplication-gouvernement-base-reconnaissance-faciale-fait-polemique_29820368.html.

[27] Considérant n° 42 du RGPD et Comité européen de la protection des données, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) n° 2016/679, 4 mai 2020, n° 3.

[28] Considérant n° 43 du RGPD.

[29] E. Debaets, *A propos des dérives actuelles du consentement en matière de protection des données - Le Conseil d'État et Alicem, in Actualité juridique de droit administratif AJDA*, 2021, n° 6, 346.

[30] Pour rappel, aux termes de l'article 9 du RGPD, les données biométriques sont qualifiées de données sensibles dès lors qu'elles servent à l'identification. Leur traitement est donc par principe interdit mais de nombreuses exceptions existent.

[31] J. Eynard, *RGPD et « empouvoirement » individuel : promesse tenue ou espoir déçu ?*, in *Revue des affaires européennes*, 2021, n° 1, juillet 2021, 15.

[32] Comité consultatif Convention 108, *Lignes directrices sur la reconnaissance faciale*, 28 janvier 2021, T-PD(2020)03rev4, 5.

[33] Conseil d'État, 10ème et 9ème chambre réunies, 4 novembre 2020, La Quadrature du net, n° 432656.

des services à distance sans nécessairement passer par l'application litigieuse et le recueil de gabarits de reconnaissance faciale[34]. Ce faisant, il omet que les alternatives en question ne permettent pas d'atteindre un niveau de garantie élevé. Pour les services requérant ce niveau de garantie, l'utilisateur se trouvait *de facto* en théorie contraint d'utiliser Alicem, à moins de se déplacer en personne.

Outre les difficultés liées au consentement, le respect du principe de proportionnalité était remis en cause. Le dispositif conçu se révélait en effet particulièrement intrusif, en raison notamment de l'inclusion de technologies biométriques. Ces technologies imposent le recueil d'informations biologiques ou comportementales considérées comme quasi uniques pour constituer des gabarits qui permettront l'identification et l'authentification. Le principe de proportionnalité, décliné en un principe de subsidiarité, impose donc de les éviter autant que possible. La Commission nationale de l'informatique et des libertés (CNIL) est allé dans ce sens dans sa délibération du 18 octobre 2018. Pour elle, « la mise en œuvre du traitement projeté doit être subordonnée au développement de solutions alternatives au recours à la biométrie, telle qu'utilisée pour vérifier l'exactitude de l'identité alléguée par la personne créant son compte, et ainsi s'assurer de la liberté effective du consentement des personnes concernées au traitement de leurs données biométriques au moment de l'activation de leur compte ALICEM »[35]. Une censure du dispositif Alicem sur le fondement d'une atteinte au principe de proportionnalité aurait donc été possible. Le Conseil d'État décide du contraire en considérant « que le recours au traitement de données biométriques (…) [devait] être regardé comme exigé par la finalité de ce traitement »[36]. Ce faisant, l'utilisation de données biométriques est considérée comme proportionnée pour atteindre l'objectif d'identification/authentification escompté.

Malgré cette décision positive du Conseil d'État, Alicem n'a jamais été déployé de sorte que ce moyen d'identification n'a jamais pu être utilisé en France par l'usager ou les fournisseurs de services. En réalité, Alicem a toujours été conçu comme un test, comme une première brique vers un dispositif qui, lui, serait largement diffusé. Ce dispositif prend le nom de Service de garantie de l'identité numérique (SGIN).

2.2. *La naissance du Service de garantie de l'identité numérique*

Le décret n° 2022-676 du 26 avril 2022[37] donne naissance au SGIN en même temps qu'il met fin à Alicem. En pratique, il crée un traitement de données à caractère personnel mis en œuvre par deux responsables conjoints étatiques, à savoir le ministre de l'intérieur (secrétariat général) et l'Agence nationale des titres sécurisés (ANTS). Ce traitement a vocation à permettre aux titulaires d'une carte nationale d'identité comportant un composant électronique d'utiliser une application téléchargée sur un téléphone portable pour s'identifier et s'authentifier électroniquement auprès d'organismes publics et privés. S'identifier en ligne nécessite par conséquent de posséder un téléphone doté de la technologie de lecture sans contact mais surtout l'utilisateur doit être titulaire d'une carte d'identité électronique alors que celle-ci n'est délivrée en France que depuis le 2 août 2022. Cette temporalité présente en réalité un avantage puisqu'il permet au dispositif « SGIN » de ne pas reposer sur un mécanisme de reconnaissance faciale à distance. Comme il prend appui sur une carte nationale d'identité dont la délivrance n'est qu'à ses débuts, le nouveau système utilise le processus d'identification et d'enrôlement mis en œuvre pour la création de la carte nationale d'identité. Ainsi, « il bénéficie des mesures mises en place pour celles-ci, et donc du contrôle visuel de l'identité du demandeur par un agent de l'État sur la base des documents fournis pour la demande, ainsi qu'une comparaison d'empreintes entre le demandeur et les données inclues dans son titre

[34] *Ibid.*

[35] CNIL, Délibération n° 2018-342 du 18 octobre 2018 portant avis sur un projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé « Application de lecture de l'identité d'un citoyen en mobilité » (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile.

[36] Conseil d'État, *La Quadrature du net*, *op. cit.*, considérant n° 8.

[37] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », JORF n° 0098 du 27 avril 2022.

biométrique »[38]. Le nouveau schéma d'identification mis en place profite du face-à-face nécessaire à l'établissement de la carte nationale d'identité pour atteindre le niveau de garantie élevé, alors que le dispositif Alicem avait suppléé ce face-à-face par le mécanisme de reconnaissance faciale.

Le traitement mis en oeuvre inclut des données permettant l'identification de l'usager telles que son nom ou son prénom, des données permettant l'identification du titre détenu par l'usager (numéro du titre, date de délivrance, …), des données relatives à l'historique des transactions réalisées par l'usager, dans la limite d'un nombre maximal de transactions déterminé par les responsables de traitement (destinataire des données d'identification personnelle de l'usager, catégorie de la transaction, statut de la transaction, …) ainsi que l'identifiant du téléphone portable.

Conformément à la logique sous-jacente au RGPD et au cadre légal entourant l'identité numérique, le fonctionnement du SGIN repose sur l'idée suivant laquelle la personne concernée doit conserver la maîtrise des informations qui la concernent. Cela se voit à plusieurs égards. Tout d'abord, le système permet à l'utilisateur d'établir des attestations de façon à ce que celles-ci n'intègrent que les seules informations utiles au service destinataire, conformément au principe de minimisation. Ensuite, l'architecture retenue implique une conservation des données par l'utilisateur ou, sous son contrôle. Un double stockage est prévu. D'une part, l'utilisateur conserve l'ensemble des informations dans son équipement terminal. D'autre part, les responsables du traitement stockent les données, à l'exception de celles relatives aux transactions, dans un serveur qu'ils gèrent. L'inutilité dans le cadre de la gestion du moyen d'identification opérée par les organes de l'État justifie que ces informations ne soient pas stockées au niveau national et restent en local, pour répondre aux besoins pratiques de l'utilisateur. De nouveau, le principe de minimisation est respecté. La conservation des données de journalisation mérite ici d'être mentionnée. D'une durée de trois ans, cette conservation s'opère dans le serveur des responsables du traitement mais les données ne peuvent être consultées que par certaines personnes et selon des modalités précises. D'une part, seuls les agents des services des responsables du traitement sécurisés chargés de la maîtrise d'ouvrage et de la maîtrise d'œuvre du traitement de données personnelles mis en œuvre dans le contexte du SGIN, individuellement désignés et spécialement habilités par leur directeur, peuvent les consulter. D'autre part, cette consultation ne peut se faire qu'à la demande de l'usager ou, en cas de litige, après l'en avoir informé[39]. Ce faisant, la personne reste au centre du dispositif mis en place, quand bien même une simple information peut suffire à l'évincer.

L'étude du fonctionnement du SGIN sous l'angle du RGPD conduit globalement à saluer le dispositif mis en œuvre. Les droits des personnes sont préservés[40]. L'accès aux données est restreint à certains acteurs. avec l'obligation pour les responsables du traitement de publier une liste des fournisseurs de téléservices qui pourraient accéder aux données par convention[41]. Les durées de conservation sont échelonnées en fonction des situations. Par principe, elle est d'au plus 5 ans à compter de la dernière vérification d'identité de l'usager du moyen d'identification électronique. Cette durée est néanmoins revue à la baisse dans plusieurs cas : soit la personne exerce son droit d'opposition en désinstallant par exemple l'application et les données doivent être effacées du serveur des responsables du traitement dès la désinstallation, soit la personne ne mène pas à son terme la création du moyen d'identification électronique auquel cas les données doivent être effacées de l'ensemble des supports à l'issue d'un délai de 2 mois, soit la personne n'utilise pas le moyen d'identification électronique pendant 2 ans et les données doivent être automatiquement supprimées[42]. Cette dernière situation implique qu'un mécanisme d'effacement automatique ait été prévu au moment de la conception du dispositif, en application du principe de *privacy by design*.

[38] CNIL, Délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'État autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », 2, paragraphe 7.

[39] Art. 5 du décret n° 2022-676 du 26 avril 2022.
[40] Art. 6 du décret n° 2022-676 du 26 avril 2022.
[41] Art. 3 II du décret n° 2022-676 du 26 avril 2022.
[42] Art. 4 du décret n° 2022-676 du 26 avril 2022.

La description ainsi faite du dispositif étatique en-cours de déploiement permet de comprendre pourquoi la CNIL a accueilli « très favorablement » le projet[43]. Le SGIN vient combler un manque : celui d'une identité numérique régalienne de niveau élevé et respectueuse de la vie privée des utilisateurs. Par son biais, l'État joue à nouveau son rôle de certificateur de l'identité des citoyens, quel que soit le monde, réel ou en ligne, envisagé. Le déploiement du SGIN doit dès lors être encouragé et son positionnement par rapport à d'autres initiatives dans lesquelles l'État joue un rôle indirect, précisé.

3. *L'État, acteur indirect an matière d'identification en ligne*

Selon toute vraisemblance, le futur verra naître un éventail de dispositifs d'identification électronique, lesquels seront mis à la disposition des personnes qui choisiront quel(s) dispositif(s) privilégier pour quel(s) usage(s). Ces moyens d'identification seront délivrés par des opérateurs privés sans que l'État ne soit jamais bien loin. Dans certains cas, il désignera lui-même les opérateurs en charge de fournir le moyen d'identification (3.1) ; dans d'autres cas, il aura recours à des tiers de confiance certifiés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) (3.2).

3.1. *Le portefeuille européen d'identité numérique fourni par des opérateurs privés mandatés*

La proposition de règlement européen modifiant le règlement eIDAS et établissant un cadre relatif à une identité numérique[44] crée un nouveau moyen d'identification, dénommé portefeuille européen d'identité numérique. Il s'agit d'un produit et d'un service « qui permettent à l'utilisateur de stocker des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service […]; et de créer des signatures et cachets électroniques qualifiés »[45]. Cet outil, censé garantir à toutes les personnes physiques et morales dans l'Union un accès sécurisé, fiable et continu à des services publics et privés transfrontaliers, devra en principe être délivré par chaque État membre dans un délai de 12 mois à compter de l'entrée en vigueur du nouveau règlement[46]. Pour le texte, l'État est donc l'acteur qui délivre le nouveau moyen d'identification. Ce principe est néanmoins vite affaibli par l'article 6 bis, deuxième paragraphe, qui dispose que le portefeuille est délivré soit par un État membre, soit sur mandat d'un État membre, soit indépendamment d'un État membre mais avec une reconnaissance par ce dernier du portefeuille délivré. Si l'État demeure le premier acteur visé, on constate que son rôle s'étiole au fur et à mesure des possibilités. Il est alors permis de s'interroger sur les critères qui seront appliqués pour octroyer un mandat ou pour reconnaître un portefeuille délivré par un organisme tiers.

Sur ce point, la proposition de règlement livre quelques pistes. Elle indique que le portefeuille doit être délivré en application « d'un schéma d'identification électronique notifié, conçu selon des normes techniques communes, et à la suite d'une évaluation obligatoire de la conformité et d'une certification volontaire au sein du cadre européen de certification de cybersécurité, tel qu'établi par le règlement sur la cybersécurité »[47]. L'organisme qui délivre le portefeuille, qu'il soit mandaté ou non, devra dès lors être en mesure de prouver qu'il a suivi un schéma d'identification électronique qui, d'une part, a été conçu selon des normes techniques communes[48] permettant d'atteindre un niveau de garantie élevé et qui, d'autre part, a fait l'objet d'une notification auprès de la Commission européenne. Au surplus, il lui faudra présenter une évaluation de la conformité ainsi qu'une certification de

[43] CNIL, Délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'État autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », 3, paragraphe 13.

[44] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021, COM(2021) 281 final.

[45] *Ibid*., 26.

[46] Nouvel Art. 6 bis 1. Introduit par la proposition de règlement, *ibid.* Ce délai est passé à 24 mois dans l'accord de principe obtenu en juillet 2023 (art. 6a 1.)

[47] Exposé des motifs, *Ibid*., 11.

[48] *The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework*, 26 janvier 2023.

cybersécurité. L'article 6 quater de la proposition vise en réalité une triple certification : celle du portefeuille en lui-même, celle liée à la cybersécurité du portefeuille et celle liée au traitement des données personnelles via le portefeuille[49]. En pratique, des procédures seront nécessaires pour que l'ensemble de ces garanties soit mis en œuvre et contrôlé. La Commission européenne prévoit en ce sens un délai de six mois à compter de l'entrée en vigueur du règlement à venir pour dresser une liste des normes de certification des portefeuilles qui seront délivrés[50]. Selon un schéma classique, des organismes seront accrédités pour procéder à la certification, si bien que des critères spécifiques devront être dégagés pour évaluer ces organismes évaluateurs et leur octroyer une accréditation[51]. On peut finalement s'attendre à ce que deux référentiels voient le jour : l'un, pour les prestataires désireux de délivrer le portefeuille et l'autre, pour les entités désireuses de certifier les portefeuilles. Pour des questions d'harmonisation, c'est la Commission européenne qui établira ces documents et non l'État membre.

Sur le papier, le schéma ainsi établi, fondé sur une triple certification de l'architecture, de la sécurité et des données personnelles devrait permettre au portefeuille d'être un moyen d'identification fiable et respectueux des droits et libertés des individus. Ceci est d'autant plus vrai que la proposition de règlement organise l'obligation pour un ensemble d'acteurs d'accepter le portefeuille comme moyen d'identification. L'article 12 ter issu de la proposition de règlement vise en ce sens les très grandes plateformes en ligne[52] ainsi que les parties utilisatrices privées qui, conformément au droit national, au droit de l'Union ou à une obligation contractuelle, exige une authentification forte de l'utilisateur, « y compris dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications »[53]. L'obligation faite aux très grandes plateformes d'accepter le portefeuille comme moyen d'identification est aussi symptomatique de la volonté de reprendre la main sur la fonction d'identification, au détriment des outils développés par les sociétés Facebook, Google (Alphabet), … La protection des droits et libertés fondamentaux assurée par le portefeuille passe par ailleurs par l'exigence de cloisonner les données. L'article 6 bis, paragraphe 7, issu de la proposition de règlement dispose à cet égard que « les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue ». De cette façon, les données d'identité ne sont pas reliées à l'historique des services, des transactions, des demandes formulées par l'utilisateur. Une étanchéité est mise en œuvre qui permet à la personne de préserver sa vie privée. Cette étanchéité interroge néanmoins.

Dans la pratique en effet, la vigilance s'impose. Si imperméabilité entre les données d'identité et les données d'utilisation du portefeuille il y a, comment le fournisseur du portefeuille se rémunère-t-il alors que la délivrance de cet outil est gratuite pour la personne[54] ? La volonté de faire supporter cette charge financière par les fournisseurs de services qui demandent aux utilisateurs de s'identifier est-elle tenable économiquement ? Si la réponse est négative, le modèle économique ne repose-t-il pas finalement sur l'exploitation des données d'utilisation du portefeuille ? Ces questions sont légitimes quand l'article 6 bis, paragraphe 7, issu de la proposition de règlement prévoit que « l'entité qui délivre le portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille qui ne sont pas nécessaires à la fourniture des services qui y sont attachés » et qu'elle « ne combine pas des données d'identification personnelle et

[49] On notera que la certification liée au traitement de données personnelles semble avoir été allégée au fur et à mesure des débats. Là où la proposition de règlement utilisait les termes « shall be certified », le dernier accord politique utilise « may be certified ». Voir l'article 6c 3) de l'accord obtenu en juillet 2023.

[50] Art. 6 quater, paragraphe 4, de la proposition de règlement.

[51] *Ibid*., art 6 quater, paragraphes 3 et 6.

[52] Telles que définies par l'article 35 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *JOUE* L 227/1 du 27 octobre 2022. Ce règlement est également appelé le *Digital Services Act* ou DSA.

[53] Art. 12 paragraphe 2 de la proposition de règlement.

[54] Art. 6 *bis*, paragraphe 6 de la proposition de règlement.

d'autres données à caractère personnel stockées ou relatives à l'utilisation du portefeuille européen d'identité numérique avec des données à caractère personnel provenant de tout autre service offert par cette entité ou de services tiers qui ne sont pas nécessaires à la fourniture des services attachés au portefeuille, à moins que l'utilisateur n'en ait fait expressément la demande ». En effet, la première partie de phrase laisse entendre que le fournisseur du portefeuille peut collecter des informations relatives à l'utilisation de portefeuille dès lors qu'elles sont nécessaires pour fournir les services attachés au portefeuille. Quels sont ces services dont il est fait mention ? En l'état, l'expression paraît si large qu'elle laisse penser que le fournisseur peut collecter un nombre important d'informations. Quant à la seconde partie de la phrase, elle pose un principe d'interdiction qui va dans le sens d'une protection forte des droits et libertés, pour affaiblir ce principe en prévoyant la possibilité de recueillir le consentement de la personne pour procéder à la combinaison des données. Pour terminer, que penser de l'identifiant unique et persistant qui doit être stocké dans le portefeuille[55] ? Les garanties posées qui consistent à permettre un changement d'identifiant à la demande de l'utilisateur et à prendre des mesures techniques et organisationnelles pour assurer un niveau élevé de protection des données à caractère personnel utilisées pour l'appariement des enregistrements et pour empêcher le profilage des utilisateurs sont-elles suffisantes ? Certes, le dernier accord de principe obtenu en juillet 2023 ne reprend pas cette idée d'identifiant unique mais il enjoint les États membres à garantir sans équivoque la concordance des identités des personnes physiques utilisant des moyens d'identification notifiés ou des portefeuilles d'identité numérique européens. La question est alors celle de savoir comment garantir cette concordance dans le respect des droits et libertés fondamentaux.

Ces interrogations laissent présager de difficultés à venir. Elles s'ajoutent à celle de l'articulation du portefeuille fourni par les organismes privés avec les outils d'identification d'ores et déjà délivrés par les États. Dans le cadre du portefeuille, les intérêts économiques en jeu sont forts, ce qui crée une inquiétude quant à l'implication des entités privées. Cette inquiétude ne semble pas si forte quand l'État recourt à des tiers de confiance certifiés comme le sont les prestataires de vérification d'identité à distance.

3.2. *L'intervention d'opérateurs privés de confiance*

En l'absence de face-à-face en mairie, l'identité doit pouvoir être vérifiée de façon fiable. Pour y parvenir, l'État recourt à des tiers dits de confiance, qui portent le nom de prestataires de vérification d'identité à distance (PVID). Ce sentiment de confiance naît de la mise en œuvre d'un cadre protecteur, dans lequel des garanties sont prévues en amont et en aval de la certification comme PVID. Reste à déterminer si ces garanties sont suffisantes.

La certification comme PVID impose, pour le candidat, de suivre une procédure d'évaluation[56] consistant à déterminer si le candidat remplit les conditions fixées dans le référentiel d'exigences établis par l'ANSSI pour le service spécifique de vérification d'identité à distance[57]. Ce document décrit les modalités de mise en oeuvre d'un service de vérification d'identité, lequel requiert une vidéo du visage de l'utilisateur ainsi que, en fonction des cas, soit une vidéo du titre d'identité présenté par l'utilisateur, soit les données d'identification relatives à l'utilisateur stockées dans le composant de sécurité du titre d'identité présenté par l'utilisateur, y compris la photographie du visage de l'utilisateur[58]. Sur la base de ces données, le prestataire doit veiller, à l'aide de traitements automatisés et humains, à ce que le titre d'identité présenté par l'utilisateur soit authentique et à ce que l'utilisateur soit le légitime détenteur du titre d'identité. Pour ce faire, une détection du caractère « vivant » de l'utilisateur présent sur la vidéo doit être effectuée. De même, une comparaison a lieu entre son visage extrait de la vidéo avec soit une photographie de son visage extrait de la

[55] Art. 11 bis de la proposition de règlement.

[56] ANSSI, *Processus de qualification d'un service, version 1.0*, 6 janvier 2017, www.ssi.gouv.fr/uploads/2014/11/qual_serv_process-processus-de-qualification-d-un-service.pdf.

[57] ANSSI, *Prestataire de vérification d'identité à distance. Référentiel d'exigences*, Version 1.1, 1er mars 2021, www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf.

[58] *Ibid*., 12 et 13.

vidéo du titre d'identité, soit la photographie de l'utilisateur extraite du composant de sécurité du titre d'identité. Les technologies de reconnaissance faciale sont ainsi mobilisées[59], de façon à pouvoir atteindre un niveau suffisant de fiabilité et bien qu'elles fassent l'objet de controverses. Ceci explique que le prestataire doive respecter un ensemble de garanties propres à assurer la fiabilité du service fourni mais aussi la confidentialité et l'intégrité des données traitées.

En application du référentiel établi par l'ANSSI, le PVID est notamment tenu d'exigences générales, d'obligations en termes d'appréciation et de traitement des risques, du devoir de prendre les mesures techniques et organisationnelles appropriées pour protéger l'information. L'article IV 1. établit par exemple une liste de dix exigences générales, portant sur la qualité de personne morale du prestataire, sur son obligation de souscrire une assurance professionnelle, sur l'apport d'une preuve suffisante attestant que les modalités de son fonctionnement ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du commanditaire ou de provoquer des conflits d'intérêts, … Une attention particulière est également portée au personnel recruté, avec l'obligation de s'assurer de la véracité des *curriculum vitae* fournis et d'organiser des moyens de sensibilisation aux risques spécifiques rencontrés par certains employés. Un nombre suffisant de personnes doit être recruté, des sessions de formation doivent être organisées et les compétences, être régulièrement évaluées. Dans sa mission, le prestataire doit pouvoir estimer les risques. Il lui est par exemple demandé de prévoir un plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité. Il est par ailleurs tenu d'élaborer et de tenir à jour une politique de vérification d'identité à distance. Le règlement général sur la protection des données (RGPD)[60] s'applique en outre à lui. En réponse à la jurisprudence de l'Union européenne[61], il est intéressant d'observer l'obligation faite au prestataire d'héberger les données relatives au service de vérification d'identité à distance au sein du territoire de l'Union européenne ainsi que d'exploiter et d'administrer ce service depuis ce territoire.

Bref, le prestataire est enfermé dans un ensemble de règles, fixées par l'État par l'intermédiaire de l'ANSSI, et relatives au service fourni mais aussi au prestataire lui-même (son organisation, les qualités qu'il doit présenter, …), qui limitent mais n'estompent pas l'inquiétude qu'un tel service de vérification d'identité peut susciter en termes d'atteinte aux droits et libertés fondamentaux. A ce jour, trois acteurs seulement ont été certifiés par l'ANSSI et seuls sept services sont à l'étude[62]. Ces derniers relèvent en outre tous d'un niveau de garantie substantiel. Aucun prestataire ne semble donc pouvoir être en mesure d'assurer un niveau de garantie élevé à court terme, sauf à supposer qu'un prestataire disposant d'un tel service n'a pas souhaité apparaître sur la liste publiée par l'ANSSI[63].

4. *Conclusions*

En conclusion, il faut observer le cheminement opéré en matière d'identification électronique à distance, avec, on peut l'espérer, une perte de vitesse des grandes plateformes, au profit de l'État, mais aussi d'entités privées certifiées, notamment par l'ANSSI. L'avenir dira lequel de ces deux acteurs, public ou privé, parvient à s'imposer en matière de certification d'identité en ligne. Si, à ce jour, l'État français semble avoir pris un peu d'avance[64] en proposant le seul moyen

[59] On notera qu'un opérateur humain peut également intervenir pour valider le caractère vivant de l'utilisateur et procéder à la comparaison demandée.

[60] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE L 119, 4 mai 2016, 1-88.

[61] Notamment l'arrêt de la CJUE du 16 juillet 2020 (affaire C-311/18, Data Protection Commissioner/Maximillian Schrems et Facebook Ireland), dit Schrems II, dans lequel la Cour invalide la décision d'exécution de la Commission européenne ayant considéré les principes du Privacy Shield comme adéquats et, ce faisant, autorisant les transferts de données personnelles vers les États-Unis sous certaines conditions.

[62] https://www.ssi.gouv.fr/entreprise/produits-certifies/prestataires-de-verification-didentite-a-distance-pvid.

[63] Le site de l'ANSSI indique en effet que « seuls apparaissent les projets de certification que les prestataires ont accepté de rendre publiques ».

[64] A l'échelle européenne, l'État français semble plutôt être en retard, au moment où plusieurs États membres ont déjà notifié un ou plusieurs schémas d'identification électronique de niveau élevé à la Commission européenne. Sur ce point, voir https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNIT

d'identification assurant un niveau de garantie élevé, la vigilance reste de mise. Le recours à des acteurs privés ne peut s'opérer qu'au prix de contrôles réguliers, visant à s'assurer de la confidentialité des données traitées, du niveau de sécurité atteint et du respect des droits et libertés fondamentaux. L'État doit encore ici jouer un rôle important, sous peine de perdre la maîtrise de l'identification en ligne de ses citoyens et de laisser cette fonction aux acteurs du marché, dont la survie dépend d'une bonne santé économique. L'identité, même lorsqu'elle est traitée sous l'angle de la certification, ne peut être appréhendée comme un objet ordinaire car, au-delà de l'instrument de police qu'elle représente, l'identité relève de l'intimité de ce que nous sommes depuis notre naissance. L'État doit en être le garant.

Y/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 145-152
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 11

*Protection of Personal Data and Digital Identity in relation to the Public Administration: Public Digital Identity System (SpID) in Italy**

Michele Martoni
(Researcher of Legal Informatics – Department of Law – University of Urbino)

ABSTRACT The Italian legislator introduced the Public Digital Identity System (SpID). This tool allows citizens and businesses to dialogue with public administrations. The use of SpID also raises questions about data protection in consideration of the information flows, the subjects involved, and the services provided. This paper outlines the interaction of digital-identities mechanism in the EU context. Finally, it addresses the issue of data protection with a focus on the use of SpID by minors.

1. *From the digital transition to the introduction of the Italian SpID*

Italy has adopted the principle of digital first[1] implemented through the provisions contained in Legislative Decree no. 82 of 2005 (Digital Administration Code or CAD),[2] according to which public administrations must manage administrative procedures using information and communication technologies, must operate through electronic documents and communicate through telematic tools, must accept electronic payments and, moreover, they must guarantee anyone the right to use the services they provide in digital form and in an integrated way, through the telematic tools made available by the public administrations themselves.

The basis of this transition is the National Resident Population Registry (ANPR) governed by Article 62, Legislative Decree n. 82 of 2005, and the related implementing decrees.[3] It is the national database into which the municipal registries will progressively converge.

The ANPR absorbs within itself the National Index of Registries and the Register of Italians Abroad (AIRE). It also contains the computerized national archive of civil-status registers kept by the municipalities, thus creating a single point of reference, a single database, for information relating to personal digital identity.

The Italian legislator, with Decree n. 69 of 2013,[4] amended by Legislative Decree no. 82 of 2005, introduced in our legal system the Public System for the management of Digital Identities (known as SpID).[5] Subsequently, the legislator intervened again, with Decree of 24 October 2014[6] and with Legislative Decrees no. 179 of 2016[7] and no. 217 of 2017[8], to adapt our system to European Regulation no. 910/2014[9] (eIDAS-electronic

* Article submitted to double-blind peer review.

[1] G. Pesce, *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, Editoriale Scientifica, 2018.

[2] www.normattiva.it/eli/id/2005/05/16/005G0104/CONSOLIDATED/20220929, last access on 28 September 2022.

[3] For more details see www.anagrafenazionale.interno.it/il-progetto/strumenti-di-lavoro/normativa/, last access on 29 September 2022.

[4] www.normattiva.it/eli/id/2013/06/21/13G00116/CONSOLIDATED/20220929, last access on 20 September 2022.

[5] About SpID, see V. Amenta, A. Lazzaroni and L. Abba, *L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al web*, in *Ciberspazio e diritto*, n. 1, 2015, 11; A. Contaldo, *La disciplina dello SpID (Sistema Pubblico di Identità Digitale) e la definizione giuridica dei gestori*, in *Rivista Amministrativa della Repubblica Italiana*, nn. 9-10, 2016, 541; S. Tura, *Il sistema pubblico di identità digitale*, Bologna, Società Editrice Esculapio, 2017. See also I. Macrì, *L'identità digitale, nuovo documento di riconoscimento*, in *Azienditalia*, n. 3, 2021, 475. See also F. Buccafurri, L. Fotia *et al.*, *Enhancing Public Digital Identity System (SPID) to Prevent Information Leakage*, in A. Kő and E. Francesconi (eds.), *Electronic Government and the Information Systems Perspective*, vol. 9265, Cham, Springer, 2015.

[6] www.gazzettaufficiale.it/eli/id/2014/12/09/14A09376/sg, last access on 10 September 2022.

[7] www.normattiva.it/eli/id/2016/09/13/16G00192/CONSOLIDATED/20220929, last access on 20 September 2022.

[8] www.normattiva.it/eli/id/2018/01/12/18G00003/CONSOLIDATED/20220929, last access on 20 September 2022.

[9] https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32014R0910&from=IT, last access on 20 September 2022. On the eIDAS Regulation, see G. Fi-

IDentification Authentication and Signature), on electronic identification and trust services for electronic transactions in the internal market.

2. *Elements for a better understanding of the SpID*

Italian legislation defines[10] the so-called "SpID digital identity" as "the computer representation of the correspondence between a user and his identification attributes, verified through the set of data collected and recorded in digital form" according to the procedures set out in the implementing decree of Article 64 of Legislative Decree no. 82 of 2005.

To understand the meaning of this definition, it is therefore necessary to refer to the implementing Decree of 24 October 2014, with the *caveat* that the terminology used in Italian law does not correspond to that used in the EU regulation.

In fact, eIDAS Regulation does not use the expression "digital identity", used by the Italian legislator, but the expressions "electronic identification", "person identification data" and "electronic identification means".

Electronic identification means the process of using personal-identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

Personal-identification data means a set of data enabling the identity of a natural or legal person, or of a natural person representing a legal person to be established.

Electronic identification means are a material and/or immaterial units containing personal-identification data, and which are used for authentication for online services.

Lastly, authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.[11]

The first definition that deserves attention is "attributes" (*identifying*, *secondary* and *qualified*), that is an information or qualities of users used to represent their identity, status, legal form, or other peculiar characteristics.[12]

The identification attributes are name, surname, place and date of birth, sex, or company name, registered office, as well as the tax code or VAT number and the details of the identity document used for identification purposes.[13] All this information, moreover, falls into the category of personal data.

The "secondary attributes" are the landline or mobile telephone number, e-mail address, physical and digital address, as well as any other attributes identified by the Agency for Digital Italy (AgID) functional to communications.[14]

Finally, the "qualified attributes" are qualifications, professional ratings and powers of representation and any other type of attributes certified by a qualified authority.[15] This information also falls into the category of personal data.

SpID's actors are the Agency for Digital Italy (AgID), users, identity provider (or IdP), attributes authority, and service provider (or SP).

AgID takes care of the activation of the SpID, carrying out, in particular, the following activities: i) manages the accreditation of the identity and attributes providers, stipulating specific agreements with them; ii) takes care of updating of the SpID register and supervises the work of the subjects participating in the SpID; iii) stipulates specific agreements with those who certify the validity of the identification attributes, that is, the verification of identity documents.

User are those who request the SpID code and who, after obtaining it, intend to access an online service.[16]

SpID identity providers (IdP) are the legal persons accredited to the SpID who, as providers of public services, after identifying the user, assign, make available and manage the attributes used by the same user for the purpose of his/her electronic identification.

The qualified-attributes providers are the subjects accredited by the AgID who have the power to certify the possession and validity of qualified attributes, at the request of service providers.[17]

The service provider (SE) provides

nocchiaro, *Una prima lettura del reg. UE n. 910/2014 (c.d. Eidas): identificazione online, firme elettroniche e servizi fiduciari*, in *Le Nuove Leggi Civili Commentate*, n. 3, 2015, 419.

[10] Translation by the author.

[11] For definitions, see Article 3(1) of eIDAS Regulation.

[12] Cf. Article 1(1)(b) of the Decree of 24 October 2014.

[13] Cf. Article 1(1)(c) of the Decree of 24 October 2014.

[14] Cf. Article 1(1)(d) of the Decree of 24 October 2014.

[15] Cf. Article 1(1)(e) of the Decree of 24 October 2014.

[16] Cf. Article 1(1)(v) of the Decree of 24 October 2014.

[17] Cf. Article 1(1)(m) of the Decree of 24 October 2014.

Information Society services[18] or services that administrations and public bodies provide users through online information systems. The SE forwards users' electronic identification requests to the IdP.[19]

I note that the IdP is qualified as a "public service provider" and that it is expressly assigned the task of carrying out users' identification.

This task is reiterated in Article 7 of Decree of 24 October 2014, which states that digital identities are issued, at the request of the interested party, by the identity provider, after verification of the identity of the applicant.

The provision then specifies the methods for verifying the identity of the applicant.

The Decree of 24 October 2014 then regulates (i) the identification code, (ii) the access credential and (iii) computer authentication, linking them to the computer (or electronic) identification procedure.

The identification code is a particular attribute assigned by the IdP which allows to uniquely identify a digital identity in the context of the SpID. This is a unique code, which is assigned by the provider of the SpID code, and which can take, for example, a format like "INFC0000052141".

The access credential is a particular attribute used by the user, together with the identification code, to securely access, through electronic authentication, the qualified services provided by suppliers of services that adhere to the SpID.[20] Article 1(1)(r), of the Decree of 24 October 2014, specifies (incidentally) that the credentials are "chosen".

Electronic authentication is the verification carried out by the IdP, at the request of the SE, of the validity of the access credentials presented by the users to the same provider, to validate their electronic identification.[21]

Article 6 of the Decree of 24 October 2014 provides that the SpID is based on three levels of authentication security:

a) at the first level, corresponding to the Level of Assurance LoA2 of the ISO/IEC DIS 29115 standards, the digital identity provider makes available one-factor computer authentication systems, such as passwords;

b) at the second level, corresponding to the Level of Assurance LoA3 of the ISO/IEC DIS 29115 standards, the digital identity provider makes two-factor authentication systems available, not necessarily based on electronic certificates, whose private keys are kept on devices that meet the requirements of Annex 3 of Directive 1999/93/EC of the European Parliament;

c) at the third level, corresponding to the Level of Assurance LoA4 of the ISO/IEC DIS 29115 standards, the digital-identity provider makes available two-factor authentication systems based on electronic certificates, whose private keys are kept on devices that meet the requirements of Annex 3 of Directive 1999/93/EC of the European Parliament.

The SpID code has its own life cycle that needs to be managed and monitored.

In particular, users must keep their attributes valid and updated.

The code may be subject to suspension and revocation, for example in the event of the user's death, termination of the legal entity, non-use for more than twenty four months, illegal use of the SpID code, contractual expiry or request of the user.

Below are two figures illustrating, respectively, the SPID application procedure and the procedure for requesting access to a service issued by a service provider.

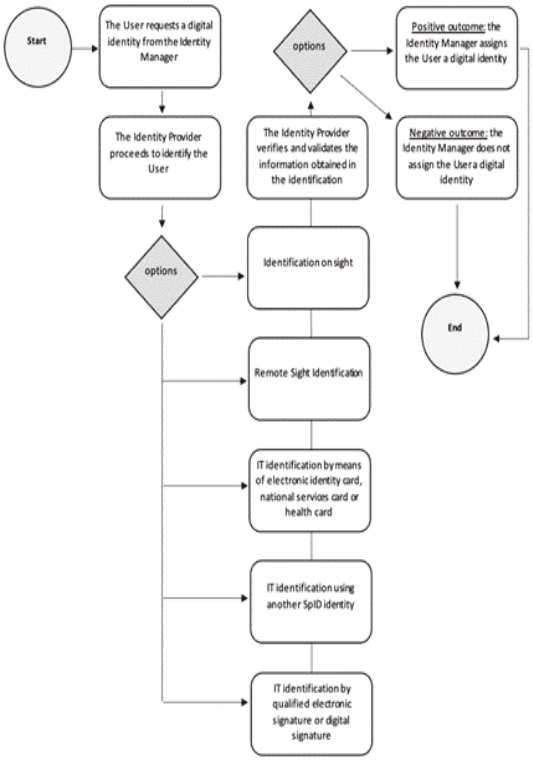

Figure 1. Application procedure

[18] Cf. Article 2(1)(a) of Legislative Decree no. 70 of 2003.
[19] Cf. Article 1(1)(i) of the Decree of 24 October 2014.
[20] Cf. Article 1(1)(h) of the Decree of 24 October 2014.
[21] Cf. Article 1(1)(f) of the Decree of 24 October 2014.

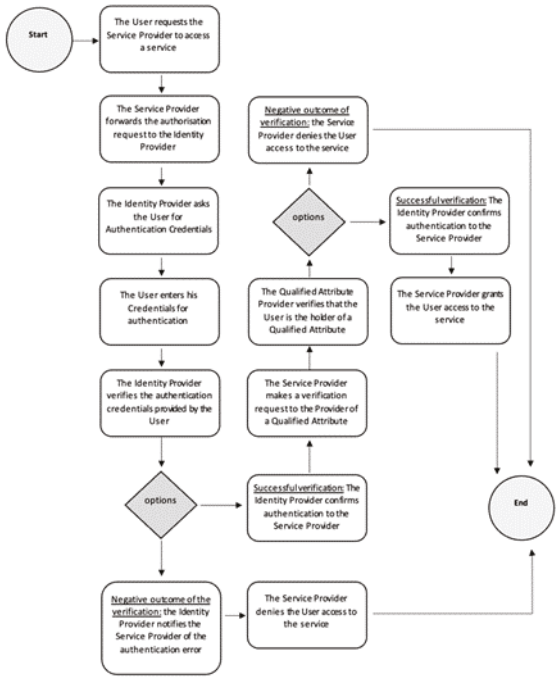

Figure 2. Procedure for service access

3. *The Italian eIDAS node (FICEP)*

The FICEP project (First Italian Cross-border eIDAS Proxy) has been financed by the European Commission under the CEF-Telecom eID 2014[22] call for proposals and is aimed at implementation of the Italian eIDAS node.

On 12 May 2017, the Directorate General for Informatics (DIGIT) of the European Commission notified AgID of the successful completion of validation tests on the correct implementation and interoperability of the national node, the implementation of which will enable the circulation of Italian digital identities (SpID) among the Member States of the European Union and *vice versa*.

Thanks to the FICEP project, with the implementation of a national eIDAS node, it will therefore be possible for Italian citizens to access the online services of other EU countries and, at the same time, for European citizens in possession of national electronic identification tools recognised under eIDAS to access the services of Italian public administrations.

The cross-border electronic identification process can be schematized as follows:

(1) the Italian user requests access to the service of an EU Member State;

(2) the service provider of the Member State sends a request to its own eIDAS node;

(3) the eIDAS node of the Member State asks the Italian user his/her country of origin;

(4) when the user selects his/her country of origin, the Member State's eIDAS node sends a request to the Italian eIDAS node; (5) the Italian eIDAS node responds to the Member State's eIDAS node's request by querying the provider of the applicant's SpID digital identity, for electronic authentication;

(6) once the electronic authentication is successful, the Italian eIDAS node sends a confirmation to the Member State's eIDAS node, which in turn forwards the confirmation to the Member State's service provider;

(7) the Member State's service provider allows the Italian user access to the requested service.[23]

4. *Instances and declarations submitted to the Public Administration by telematic means*

The Digital Administration Code provides a broad definition of services that can be delivered online, which are qualified as any service of a public administration that can be used at a distance by electronic means.[24] What these services are is not, however, indicated with a precise listing.[25]

Article 65 of the Italian Digital Administration Code (CAD) regulates the validity of instances and declarations submitted electronically to public administrations and public-service providers in general.

The Italian legislator has regulated how the telematic application must be formulated to be valid.

The first case considered by the Italian legislator requires the instance or declaration to be signed by one of the methods set out in Article 20 (CAD), which regulates the different types of electronic signatures.

Instances and declarations submitted

[22] See *www.agid.gov.it/it/piattaforme/eidas/progetto-ficep*, last access on 10 September 2022.

[23] See http://www.agid.gov.it/it/piattaforme/eidas/progetto-ficep, last access on 20 September 2022.

[24] See Article 1(1)(n-*quater*) of Legislative Decree no. 82 of 7 March 2005.

[25] On the use of information technology in the provision of public services, see A.G. Orofino and F. Cimbali, *L'uso delle tecniche informatiche nella prestazione di servizi pubblici*, in *Giurisprudenza Italiana*, n. 6, 2022, 1507; M. Martoni, *Servizi online della pubblica amministrazione: l'informatizzazione della dichiarazione di inizio attività in materia edilizia*, in *Ciberspazio e Diritto*, n. 11, 2010, 5.

electronically to the public administration are also valid when the applicant or declarant has been identified through the Public Digital Identity System (SpID), or through the Electronic Identity Card (CIE) or the National Services Card (CNS).[26]

Article 65 (CAD) provides that instances and declarations are valid even if: formed through the telematic access point for mobile devices referred to in Article 64-bis of the CAD; or signed and submitted together with a copy of the identity document; or if transmitted by the instant or declarant from his/her digital domicile registered in one of the lists referred to in Article 6-bis, 6-ter or 6-quarter (CAD) or, in the absence of a registered digital domicile, from an electronic address elected as a certified electronic mail service or a qualified certified electronic delivery service, as defined by the eIDAS Regulation.

5. *The Italian Data Protection Supervisory Authority about SpID*

The Italian Data Protection Supervisory Authority has intervened on several occasions on the SpID regulation.[27] Eight opinions have been issued since 2014. Among others, I would point out, in particular: the opinion on a model convention scheme for private service providers (29 September 2016); the opinion on a model convention scheme relating to the adherence to SpID by public administrations, in their capacity as service providers (18 February 2016) and the opinion on a draft regulation on the implementing modalities for the implementation of SpID and a draft convention relating to providers (17 December 2015); the opinion on two draft regulations containing, respectively, the implementing modalities for the implementation of SpID and the related technical rules (4 June 2015); the opinion on an outline of regulations setting out the procedures necessary to enable digital-identity providers, through the use of other IT identification systems that comply with SpID requirements, to issue digital identities (23 April 2015); the opinion on an outline of regulations setting out the procedures for the accreditation and supervision of digital-identity providers (23 April 2015); and, finally, the initial opinion on the outline of the decree of the President of the Council of Ministers on the public system for managing the digital identity of citizens and businesses (19 June 2014).

On 17 September 2020, the Italian Supervisory Data Protection Authority issued a further opinion on the new methods for issuing digital identities through remote recognition, which no longer require the simultaneous presence of the SpID operator and the applicant.

As I have already illustrated, the use of SpID implies the processing of personal data both at the time of registration and at the time of access to services.

I have also tried to graphically represent how SpID implements a flow of information – including personal data– involving various public and private entities.

This implies the need for a deep analysis during implementation for the correct allocation of roles (for example data controller and data processor) with respect to the figures envisaged by the GDPR, both regarding the identity provider and the service provider or attribute provider. This allocation of roles will have to find its own regulation in legal acts between the parties involved, and an adequate level of information and transparency with respect to the data subject will also have to be guaranteed.

It will also be necessary to ensure compliance with the fundamental principles[28] of data processing at every stage of the process.

One issue that emerges is the quantity and quality of data shared between identity providers and service providers. The proper implementation of the principles of necessity and data minimisation requires, in fact, that only data that are strictly indispensable with respect to the purpose of the processing set by the data controller should be exchanged between the two parties.

Providers must also guarantee, among other things, the principle of confidentiality and the

[26] See M. Martoni, *Identità personale anagrafica (autorizzata) vs identità personale autorappresentativa (manifestata)*, in *Rivista Trimestrale di Diritto e Procedura Civile*, n. 1, 2020, 179; M. Nastri, *Identità personale, identità digitale e identificazione elettronica alla luce del decreto semplificazioni*, in *Notariato*, 6, 2020, 608; F. Arcieri, M. Ciclosi, A. Dimitri, *et al.*, *The Italian Electronic Identity Card: overall Architecture and IT Infrastructure*, in F. Nardelli and M. Talamo (eds.), *Certification and Security in Inter-Organizational E-Service*; in *IFIP On-Line Library in Computer Science*, vol. 177, 2005.

[27] https://www.garanteprivacy.it/temi/pubblicaamministrazione-e-trasparenza/spid, last access on 28 September 2022.

[28] See Article 5, GDPR.

principle of data integrity by adopting appropriate and adequate security measures in this respect.

I will not dwell further on these general profiles. Rather, I would like to direct my attention to a particular implementation of the SpID that raises issues regarding the processing of personal data. I intend to refer to the possibility of assigning the SpID digital-identity to minors.

5.1. *SpID and protection of Children's Personal Data*

With Determination no. 353 of 3 May 2021, AgID issued the operational guidelines for the use of SpID services by children concerning the issuance of digital identities and related methods of use for accessing online services. At the same time, AgID also launched a public consultation on the text of the guidelines, which ended on 14 June 2021.[29]

On 2 February 2022, the Italian Data Protection Supervisory Authority delivered to AgID its opinion on the draft guidelines[30] with the aim of outlining guarantees for the use of SpID by children.[31]

On 3 March 2022, AgID adopted Determination no. 51, which ultimately adopted the operational guidelines for the use of SpID services by children.[32] Subsequently, with Determination no. 133 of 11 May 2022, AgID issued some changes by publishing a second version of the guidelines.[33]

More specifically, the guidelines define: (i) how to issue a digital identity to the child; and (ii) how to use online services through this identity.

About (i) I describe below the procedure for issuing SpID in favour of a child:

(1) The IdP (Identity Provider) offers its users a service dedicated to the request for the issue of SpID in favour of children and provides specific information on the processing of the minor's personal data for the purpose of issuing and managing the digital identity, pursuant to Articles 12 *et seq.* of the GDPR;

(2) The parent, among other things, accesses, with level 2 credentials, the service made available by the IdP; enters the data relating to the minor for whom SpID is being requested (name, surname, tax code, date of birth) and declares that he/she exercises parental responsibility over the child;

(3) the IdP generates the "parent code" and then the "verification code" assigned to the child, then communicates it to the parent;

(4) the parent communicates the verification code to the child outside the IdP channels. The child communicates the verification code to the IdP;

(5) the IdP verifies the parent's authorisation to issue the SpID and, if positive, identifies the minor, verifying the correspondence of his/her identity with the data previously provided by the parent. The IdP then issues the digital identity to the minor and sends a notification to the parent, indicating the name of the minor for whom the SpID has been issued.

Let me now turn to point (ii). In this regard, AgID emphasises that service providers – before providing a service to children through SpID– must make an independent, reasoned, and demonstrable assessment of the need to:

[29] For more on the public consultation see https://docs.italia.it/AgID/documenti-in-consultazione/lg-spid-minori-docs/it/bozza/index.html, last access on 29 September 2022.

[30] For the Opinion of the Italian Data Protection Supervisory Authority www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9744322, last access on 29 giugno 2022.

[31] In his opinion, the Supervisory Authority for the Protection of Personal Data requested AgID to amend the scheme by introducing additional guarantees, particularly regarding the procedure for issuing SpID identities by Identity Providers. The Authority requires an accurate verification of the identity of the parent and the child and the identification of the information to be collected and stored, in compliance with the principle of minimisation. Service Providers will also have to undertake to assess which services to offer directly to minors and the guarantees to be ensured in view of their characteristics. The use of SpID for children under the age of 14 (and from the age of five), is only admissible for online services offered by schools (such as, for example, the electronic register) and will have to take place for an experimental period, until 30 June 2023, while still guaranteeing access to these services without SpID with the methods that may already be in use. At the end of the trial, which will also involve the Ministry of Education, the adequacy of the measures adopted will have to be assessed. Moreover, the information addressed to minors, in accordance with what is already provided for in Article 12 of the GDPR, will have to have simple and clear language. AgID will also have to send a report to the Supervisory Authority on the use of SpID by minors, indicating the services offered, the number of identities issued, any critical issues detected, and the measures identified to remedy them. For further details, see the text of the opinion already mentioned and referred to in the previous footnote.

[32] For Determination no. 51 of 3 March 2022, see https://trasparenza.agid.gov.it/index.php?id_oggetto=28&id_doc=123125, last access on 29 august 2022.

[33] For Determination no. 133 of 11 May 2022, see https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_123194_725_1.html, last access on 29 august 2022.

(a) know the minor's age; (b) obtain certainty of the user's identity for the purposes of the service.
Chapter nine of the guidelines dedicated to the protection of personal data, specifies that AgID's indications are explicitly oriented towards the concrete application of the principles underlying the protection of personal data under Article 5 of the GDPR, the procedures identified for the issue and management of the child's digital identity and for the use of the services.
With a view to maximum protection of the child's personal data, SpID allows service providers –when they deem it appropriate based on their own evaluations, in compliance with the principle of accountability– to obtain certainty as to the age of the child even in the absence of any other data that could further identify him/her. The SE could, for example, request only the attribute attesting to the minor's date of birth without any other identifying information.
This would make it possible, on the one hand, to verify that a child is not accessing inappropriate content but, at the same time, it would make it possible not to expose him or her to data processing resulting from the use of the service for which he or she would essentially be anonymous. This modality is in the groove already traced by the CNIL[34] and the ICO.[35]

6. *An evolving scenario*

The European Commission presented on 3 June 2021 a proposal to amend the eIDAS Regulation with which it aims to introduce the so-called *European Digital Identity Wallet.*[36]
The European Digital Identity Wallet would combine, in a mobile environment, the national electronic identification solutions – introduced so far by the Member States in implementation of the eIDAS Regulation– with the digital attestation of personal attributes (e.g., possession of a driving licence, educational qualifications, medical prescriptions).
The proposed regulation will therefore impose an obligation on Member States to develop their own solution based on common technical interoperability and security standards that the Commission will publish within six months of the entry into force of the amendment to the Regulation.
The existing legal framework for digital identities, i.e., the current version of the eIDAS Regulation, provides the basis for cross-border electronic identification, authentication, and certification of websites within the Union.
However, there is no obligation for Member States to develop a national digital ID and make it interoperable with those of other Member States, which leads to large discrepancies between countries.
Hence the sense of the current Commission proposal that attempts to address these shortcomings by improving the effectiveness of the framework and extending its benefits to the private sector and mobile use.
The use of the European Digital Identity Wallet –according to the intentions of the Commission proposal– is to be used with respect to (i) the public administrations of the Member States, even if the European Digital Identity Wallet is issued by another Member State, (ii) private service providers using strong authentication systems by virtue of legal or contractual obligations, and, finally, (iii) large digital platforms (as they will be better defined in the Digital Service Act[37]).
The new Wallets will therefore allow all Europeans to access online services without having to use private electronic identification

[34] See www.cnil.fr/en/home, last access on 29 September 2022.
[35] See https://ico.org.uk, last access on 29 September 2022.
[36] For the proposed amendment, see https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52021PC0281, last access on 11 September 2022. For further study see also https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en, last access 11 September 2022. In this context, it is worth mentioning the Commission's strategy called *Digital Compass 2030* (see https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en, last access on 29 September 2022. See also https://futurium.ec.europa.eu/en/digital-compass, last access on 25 September 2022. Among the targets of the strategy, 80 per cent of citizens should use an eID solution in 2030.
[37] On 24 March 2022, a provisional political agreement was reached between the Council and the Parliament on the regulation of digital markets. Approval by Coreper followed on 15 June 2022. The current text is available at: https://data.consilium.europa.eu/doc/document/ST-9342-2022-INIT/x/pdf, last access on 29 September 2022. It will apply to all online intermediaries providing services in the EU. As the obligations introduced are proportionate to the nature of the services concerned and adapted to the number of users, very large online platforms and online search engines will be subject to stricter requirements.

methods or share (where not necessary) personal data.
On the other hand, if on the one hand the use of the European Digital Identity Wallet will minimise the need to communicate users' personal data to digital service providers, on the other hand the creation of a single system containing not only the digital identities of European citizens and residents within the European Union, but also other personal data (including special categories of personal data) and documents, will pose the need to ensure a very high level of security to avert the risks of access and misuse of information and identity theft.
It is interesting to mention the European project Electronic Identification and Trust Services for Children in Europe (euCONSENT).[38]
It was financed in the Programme Pilot Project and Preparatory Actions (PPPA-2020), dedicated to the implementation of child rights and protection mechanisms in the online domain based on the GDPR and other relevant EU legislation.
The objective of the project is to establish an interoperable technical infrastructure dedicated to the implementation of child-protection and parental-consent mechanisms based on EU legislation.
The technical measures will be based on the use of electronic identification means (in particular, electronic identification schemes notified by the Member States under the eIDAS regulation).
To do this, the euCONSENT project aims to carry out a large-scale mapping of existing age verification and parental consent collection methods in the context of online child protection.
Mapping should allow the identification of good practices, including those that ensure compliance with the current regulatory framework.
Subsequently, based on a mapping evaluation, the project will focus on designing, implementing, and testing an interoperable infrastructure for online child protection, including age verification and collection of parental consent of users of video-sharing platforms or other similar online services, using different approaches.

[38] For further details on the project euCONSENT, see https://euconsent.eu, last access on 20 September 2022.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 153-160
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 12

*Regulating Behaviour on Data Platforms: The Online Restraining Order as an Administrative Measure**

Berdien B.E. van der Donk
(PhD in Law at the Centre for Private Governance, University of Copenhagen, Denmark)

ABSTRACT Data platforms assert great influence over data. The personal data of their users is used to fund the service through the sale of personalized advertisements. Though, more important for society, these platforms exert great power over the dissemination of available information. Data platforms are increasingly used to communicate with other (like-minded) people. It is a platform where information and opinions are shared. In that sense, platforms are not only the guardians of users' personal data, but also the gatekeepers of (public) information.
Access to data platforms is traditionally governed by the platforms themselves. Platforms can dictate who gets access, which content can be shared, and the grounds for a (temporary) expulsion from the platform. Despite the discussion on whether data platforms should be regulated as public utilities, or whether the operators must obey norms of fundamental rights as de facto public spheres, the direct influence of states on access to data platforms has been limited. Recently, a (political) discussion has arisen in the Netherlands as to what extent administrative bodies should be able to impose administrative measures in online spaces. In the Netherlands, access to physical places can be limited by administrative measures imposed by a municipality's mayor. Could mayors similarly impose online restraining orders, limiting a person's access to a data platform?
This article discusses online restraining orders as an administrative measure. After a short introduction to the Dutch online restraining order, the article first discusses the traditional private-governance framework to access a data platform. In this first part, the normative online order set by platforms through their terms of service is discussed. After this contextualisation, the legal grounds to impose administrative measures under Dutch law are described, followed by a discussion on the online applicability of these powers, and a discussion on the transposability of physical legislation to online spaces. Lastly, the article concludes with a reflection on the future of online restraining orders.

1. *Introduction*

In November 2021, mayor Sharon Dijksma of the city of Utrecht imposed one of the first *online restraining orders* in the Netherlands.[1] The subject, a 17-year-old citizen of the municipality, had been arrested that same day for incitement to violence on a data platform. He had urged others in a Telegram-messaging group to (violently) demonstrate against government policies on covid-19, and the banning of fireworks.[2] Following his arrest, Dijksma imposed an online restraining order, which meant that the minor had to abstain from online statements that could lead to disorder in the city of Utrecht, such as further calls to disturb public order.[3] Failure to comply with the order would result in an administrative fine of 2.500 euro. After an unsuccessful appeal, the online restraining order was revoked by Dijksma in June 2022, because there was no longer a risk of recidivism.[4]

Dijksma's action led to a political and legal academic discussion in the Netherlands on whether powers of mayors to maintain the public order in their municipality (should) extend into the online space. Currently, as will be elaborated below, Dutch mayors can impose restraining orders with effect in the

* Article submitted to double-blind peer review.

[1] The terminology 'online restraining order' reflects the Dutch terminology of *online gebiedsverbod*, which follows the stance on the discrepancy in terminology (Internet prohibition/digital restraining order) as discussed by W. Bantema, S. Twickler and S. Vries, *Juridische Grenzen En Kansen Bij Openbare-Ordehandhaving. Een Onderzoek Naar Mogelijkheden van de APV Voor de Aanpak van Online Aangejaagde Ordeverstoringen*, 2022, 13.

[2] RTV Utrecht, 26 November 2021, *Meer aanhoudingen voor opruiing, 17-jarige jongen riep op tot vuurwerkprotest in Utrecht*, www.rtvutrecht.nl/nieuws/3231139/meer-aanhoudingen-voor-opruiing-17-jarige-jongen-riep-op-tot-vuurwerkprotest-in-utrecht (accessed 28 November 2022).

[3] RTV Utrecht, 26 November 2021 'Jongen (17) uit Zeist die op sociale media opriep tot rellen krijgt "online gebiedsverbod"', www.rtvutrecht.nl/amp/nieuws/3232804/jongen-17-uit-zeist-die-op-sociale-media-oprie p-tot-rellen-krijgt-online-gebiedsverbod (accessed 28 November 2022).

[4] S. Dijksma, *Letter to the municipal council: decision on appeal 'online restraining order*, 15 June 2022, accessible at: https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Online_aangejaagde_openbare_orde_verstoringen/Raadsbrief_Beslissing_op_bezwaar__online_gebiedsverbod___1_.pdf (accessed 28 November 2022).

physical world as an administrative measure.[5] However, it is unclear whether these competences apply equally into the online sphere.[6] Following Dijksma's online restraining order, two political parties questioned whether such online measures fall within the power of mayors to impose administrative measures. Minister Yeşilgöz-Zegerius of Justice and Safety answered questions posed by the Dutch parliament on the topic.[7] Rather than providing clarity, the minister's answers demonstrated that it is uncertain whether mayors can impose online measures. Following this, also the mayor of Amsterdam announced her intention to start experimenting with online restraining orders as of October 2022, followed by similar calls in Rotterdam and The Hague.

Whether there is a legal ground for imposing these online restraining orders remained unclear, until one of these orders was recently challenged before a Dutch court.[8] The District Court judged the imposition of an online restraining order unlawful, as the current definition of the 'public space' as defined in the applicable Utrecht local order does not explicitly include online Telegram messaging-groups. However, the discussion is far from settled. In Belgium, the General Police Regulations has been updated and now includes a specific competency to impose online measures. Contrarily to the Dutch example, the Belgian 'public space' now explicitly includes virtual spaces.[9]

To create a solid basis for further (European) discussion, this article will discuss several aspects of online restraining orders to answer the question of whether public bodies can preventively impose an online restraining order, meaning that specific persons are denied access to (certain parts of) an online platform. The article starts with an overview of the current infrastructure of platforms and their private-law character. Secondly, the online restraining order will be placed in its Dutch legislative context. To do so, a short outline is given of the competency to impose administrative measures under Dutch law. Thirdly, the online applicability of administrative measures is scrutinised, leading to a discussion on the difficulty of transferring existing rules to the online sphere, namely whether the physical world and the online world are comparable enough to impose equal restrictions. Lastly, the previous topics will be discussed in conjunction to reflect on the future of online restraining orders.

2. *Private governance through social media's terms of service*

Data platforms are private companies. As such, just like any other private company, the use of their property and service is managed through contracts – in this case more specifically through the terms of service that users agree to when signing-up to the service.[10] The terms of service dictate the

[5] Administrative measures, such as a restraining order, do not legally qualify as sanctions under Dutch law. Sanctions serve as punitive measures, such as fines imposed by the police for speeding. An administrative measure containing a restraining order has a preventive character. This differentiation does not play any further role in this article.

[6] See for example the first overview study from 2018: W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau, & W.P. Stol, *Burgemeesters in cyberspace: Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*, The Hague, Sdu Uitgevers, 2018. The study was recently followed up, see: W. Bantema, S.M.A. Twickler, S. de Vries, *Juridische grenzen en kansen bij openbare-ordehandhaving Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen*, 2022, DOI:10.13140/RG.2.2.24170.80329. See also M. Buitenshuis and B. Roozendaal, *De burgemeester: burgervader, handhaver, sheriff van het internet?*, *Nederlands Genootschap van Burgemeesters*, 48, 2022, 9, where it is pointed out that lacking jurisprudence in the field of administrative law and a law that was drawn-up with only the physical world in mind, creates uncertainty.

[7] The official questions (in Dutch) submitted by the parliament and the answers (28 January 2022) can be accessed here: https://open.overheid.nl/repository/ronl-c059703af332123ceec01db41873cf82776b6d94/1/pdf/antwoorden-kamervragen-over-het-bericht-jongen-17-krijgt-allereerste-online-gebiedsverbod-in-nederland-maar-wat-betekent-dat-eigenlijk.pdf (last accessed 28 November 2022).

[8] *District Court Midden-Nederland* (2023) ECLI:NL:RBMNE:2023:375.

[9] Gemeenschappelijk Algemeen Politiereglement (General Police Regulation), §5: "For the purposes of this regulation, the term 'publicly accessible space' includes not only physical spaces but also virtual spaces accessible to the public, such as social media accounts, forums, and other digital platforms that are not limited to a small number of individuals who share common interests.", www.politie.be/5341/sites/5341/files/downloads/APR_pzzuid_2020.pdf accessed 6 December 2022.

[10] Although it has been empirically proven that users do not read the terms of service, and if they did, they would not be able to understand them, see on this J.A Obar and A. Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services'*, *SocialScience Research Network 2018*, SSRN Scholarly Paper ID 2757465 https://papers.ssrn.com/abstract=2757465 accessed 21 September 2021; and U. Benoliel and S.I Becher, *The Duty to Read the Unreadable*, in *Boston*

scope of the service, what can and cannot be shared on the platform, the sanctions for breaching the terms of service, and the redress mechanisms for decisions to remove content or user profiles.[11] Platforms are free to one-sidedly decide what should be included in the user terms and exert normative power over the scope of freedom of expression on their platforms.[12] As such, platforms can decide that also content that would otherwise fall within the scope of the freedom of expression, is to be deleted from their services. If that is the case, a user can solely complain over a *wrongful-moderation* decision – a removal by a platform in violation of (the process stipulated in) the user terms.[13] Normative, but justifiable moderation decisions are – in principle – unopposable.

Thus, the decision to offer a service to a person, to delete content, or to suspend and/or terminate a user account is governed by the rules set out by the data platform in its terms of service. However, data platforms are not fully free to decide their terms of service in the way they please. They must adhere to national law and as such, they are obliged to follow orders to delete illegal content. If the law prescribes that a person charged with or convicted of a certain crime should be suspended from their services, platforms must comply. Obligations on data platforms to remove illegal content have been increasing over the last years, both on a national level and on a European level,[14] and through numerous codes of conducts.[15]

Online restraining orders add a new dimension to the restrictions on data platforms. However, data platforms will not be affected much by these administrative measures, as the enforcement of these measures lies equally in administrative hands.[16] The online restraining order issued by Dijksma puts no additional enforcement obligation on online platforms. However, the users of these platforms do face an increase in restrictions. Not only can users be denied access to the platform based on the (normative) restrictions outlined in the terms of service, but their behaviour online can also trigger administrative measures.

3. *A mayor's competencies under Dutch administrative law*

The imposition of the online restraining order as issued by Dijksma is problematic since the legal ground on which the online restraining order was based is aimed and intended for use in *physical spaces*. As such, it does not only challenge the exclusiveness of data platforms' power as private companies, but it does so without a sound legal basis. Administrative measures are used to deter (potentially) criminal behaviour and to sustain *public order*.[17] As such, they differ from criminal sanctions as their administrative counterparts can be used fully preventively. The application of administrative measures is aimed at quick intervention, for example in the case of football hooligans or violent demonstrations.

College Law Review, vol. 2019, 2255.

[11] The new Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 ona Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) 2022 (OJ L) regulates the transparency and obligations to enforce such terms. For example, users must be presented with the reason of why content or an account has been suspended and/or terminated and be presented with the redress possibilities.

[12] See previously by the author: B. van der Donk, *The Freedom to Conduct a Business as a Counterargument to Limit Platform Users' Freedom of Expression*, in S Hindelang & A Moberg (eds.), *YSEC Yearbook of Socio-Economic Constitutions 2021: Triangulating Freedom of Speech*, Cham, Springer, 2022, 33.

[13] See for examples of successful claims in Italy: *Corte appello L'Aquila (Correggiari)* [2021] n. 1659/2021; *Tribunale di Bologna sez II (De Gaetano)* [2021] RG 5206/2020. In the Netherlands, a successful reinstatement request for a user account was based on (lack of) transparency: *District Court Noord-Holland (Van Haga/LinkedIn)* (2021) ECLI:NL:RBNHO:2021:8539.

[14] National obligations can increase the removal of content, for example the Network Enforcement Act in Germany. See on European legislation for example the European Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [OJ L 136]; Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

[15] The EU Code of conduct on countering illegal hate speech online 2016; European Commission, Code of Practice on Disinformation 2021; European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation.

[16] The enforcement of administrative orders in the Netherlands lies with the police, who are under the mayor's authority, as opposed to the restrictions outlined in the terms and conditions and the restrictions outlined therein which are to be enforced by the platform itself.

[17] According to settled case-law, public order must be interpreted as "*orderly conduct of community life"* or "*the normal conduct of business in or adjacent to a public space",* see Dutch Council of State, case of 12 November 2014, ECLI:NL:RVS:2014:4117, §6.1; and Dutch Supreme Court, case of 30 January 2007, ECLI:NL:HR:2007:AZ2104.

The power to impose administrative measures is outlined by the Dutch *Municipal Act* ('Gemeentewet'[18]). The general description of the mayor's tasks in article 172(3) charges the mayor with the burden to maintain public order in the municipality. In addition to this general competence, the mayor can impose various specific orders against individuals (article 172a sub 1), such as area bans, assembly bans, or curfews. As part hereof, the mayor can include an order for incremental penalty payments based on article 125. These specific competences have been added to the Municipal Act in 2010 as measures to curb disturbances by football hooligans and loitering by minors. To impose an area ban or an assembly ban, the individual must have been involved in (a) serious or repeated disturbance(s) of the public order in the municipality, and simultaneously, a serious risk must exist for repetition of such disturbances. These orders can last a maximum of three months and can be extended three times. The maximum duration of an area ban or an assembly ban is therefore nine months. When the reasonable threat for public order no longer persists, the ban must be revoked.

The application and interpretation of the scope of these competences is strict. Outside the scope of these articles, the mayor cannot impose measures unless these are prescribed by a municipal ordinance and have been adopted in accordance with the principle of legality.[19] That leads to the legal uncertainty as to whether mayors can impose *online measures*, such as an online area ban since the law currently does not mention that these powers can be exercised in an online environment.

[18] The full text of the *Gemeentewet* in Dutch (valid as of 5 November 2022) is available at https://wetten.overheid.nl/BWBR0005416/2022-11-05 (accessed 6 December 2022).

[19] Neither of the municipalities which are experimenting or wanting to experiment with online restraining orders have included such specific sanctions in their municipal ordinances. It is unlikely that any municipal council could 'simply' add an online ban to their municipal ordinance. An online ban would presumably limit the freedom of expression (or other constitutional rights for that matter) in a way that goes beyond what was intended by the legislator. As such, a formal law by the legislator is needed before local administration can initiate subordinate legislation. See on this discussion Bantema, Twickler and Vries (n 1), p. 27-28. This would mean a legal basis must be created by the Dutch Parliament, before online area bans can be included in a municipal ordinance.

4. *Imposing online administrative measures*

In the case of Dijksma discussed in the introduction, the online restraining order she imposed consisted of an order for incremental penalty payments (2.500 euros) prohibiting the individual from using data platforms for incitement with an effect in the municipality of Utrecht during the indicated period. The decision was described as an *'online area ban'* by the mayor herself and later by the Municipal Council. The measure aimed to prevent a further escalation of demonstrations in the city of Utrecht, which falls within the description of the mayor's tasks. However, the exact legal basis to impose the restraining order in an *online context* – if there is one at all – has led to debate.

Dijksma refers to articles 125 sub 3 of the Municipal Act ('competence to impose incremental penalty payments'), which can be relied on 'to enforce rules which belong to the tasks of the mayor'. The general description in article 172 describes these tasks as 'maintaining public order'. The only requirements included under article 172 are, firstly, that a disturbance of public order or serious fear of such disturbance must exist, and secondly, that the order must be necessary to maintain or restore public order. Both requirements were met. Dijksma highlights that the individual breached the municipal ordinance and as such, the first requirement of article 172 was fulfilled. Furthermore, the incitement to violent demonstrations affected the public order in the city of Utrecht. As such, the online restraining order would stand the test. However, whether article 172 provides a solid legal basis to impose administrative measures or merely describes the general tasks of a mayor is disputed.[20] Whether *the effect* of online behaviour in a physical place forms a sufficient base to broaden the scope of the legal powers of the mayors to the online sphere is equally unclear, but this way forward seems plausible.[21]

[20] W. Bantema, S. Twickler and S. Vries, *Juridische Grenzen En Kansen Bij Openbare-Ordehandhaving*, 6, outlining the current discussion. It is argued that article 172 only describes the general tasks of mayors and does not infer any actual competences to act and as such cannot serve as a basis for an administrative sanction.

[21] Mayors can limit communication channels to prevent a disturbance of the public order, see Bantema, Twickler and Vries (n 2), p.70-71. The measure may not make any effective communication impossible, which is unlikely the case in the way the online restriction had been formulated by Dijksma.

Nevertheless, article 172a forms a problematic base for an online sanction. An area ban can only be imposed on or near "*one or more designated objects within the municipality, or in one or more specified areas of the municipality."* Firstly, one could wonder whether the Internet as a whole, or data platforms in particular, are located *within* the municipality. Secondly, the legislative text is solely aimed at the physical world ('objects' and 'areas'), which does not automatically translate to the online world.[22] Equally as set out above, *the effect* of the online behaviour is felt within the municipality, though whether that is sufficient to conclude that the requirement of 172a is met, is quite a stretch of the legal text. In the decision on appeal, the mayor expressed the view that "the mere fact that the behaviour takes place online does not mean that it does not violate the municipal ordinance. What matters is the effect of the behaviour (the desire to cause riots) and that effect is aimed at a physical location in Utrecht. The measure can therefore be upheld (legally). There is no (unjustified) infringement of fundamental rights (including the freedom of expression)"[23] Previously, Dijksma highlighted in answers to the municipal council that the online space does not abide by territorial borders. According to her, the targeted effect within the municipality serves as a sufficient basis to fulfil the territoriality requirement. That same view is reflected in the wording of the online restraining order, which solely consists of an order to refrain from online statements aimed at disrupting public order *in the city of Utrecht*. The individual remains free to use data platforms for any other communicative purposes, including similar expressions aimed at other municipalities over which mayor Dijksma does not govern.

In a 2022-study on online restraining orders, Bantema argued that online restraining orders limit the freedom of expression of platform's users. Opposed to a physical area ban, an online area ban does not only restrict an individual's freedom to be in a certain place, but it also limits the user's possibilities to communicate and express him- or herself. One could imagine that if a mayor would be given unlimited, broad competence to limit the access to (parts of) the Internet, individuals would be limited in their possibilities to express themselves. However, from the example of Dijksma's online restraining order in the municipality of Utrecht, it follows that an online administrative measure does not necessarily restrict an individual more than a similar traditional administrative measure in the physical world would. In the example, the individual's restriction to express himself on a data platform was solely limited to the behaviour distorting public order, namely the incitement to (violently) demonstrate with an effect in Utrecht.

In February 2023, the Dutch District Court *Midden-Nederland* decided on the legality of the online restraining order imposed by Dijksma. Firstly, the court argues that an online Telegram messaging-group does not fall within the legal definition of a 'publicly accessible place' in the applicable Utrecht local order.[24] Secondly, the court affirms that Dutch law does not explicitly grant mayors the power to restrict expressions on social media platforms, which the court argues would be the effect of an online restraining order. The local order cannot serve as a basis for a restriction of freedom of expression as protected in the Dutch Constitution.

Despite this, and whilst the reasoning of Dijksma shows the best intentions to keep the municipality safe and to sustain the public order, an explicit legal basis to impose an online administrative measure does not exist. The latter requires an unjust stretch of the current provisions and as such contravenes the principle of legality. As such, the best way forward seems an update of Dutch law that reflects and includes specific competences for

[22] *Ibid*, 30.

[23] S. Dijksma, *Letter to the municipal council: decision on appeal 'online restraining order,* 15 June 2022, accessible at: https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Online_aangejaagde_openbare_orde_verstoringen/Raadsbrief_Beslissing_op_bezwaar__online_gebiedsverbod___1_.pdf (accessed 28 November 2022) (translation by the author).

[24] District Court Midden-Nederland (2023) ECLI:NL:RBMNE:2023:375, §4: "It cannot be inferred from the [local order] or its explanatory notes that it is intended to designate (also) a digital platform such as a group chat on Telegram as a "public place". This is also logical, because although a group chat (accessible to everyone) on Telegram is public, it is not a place within the meaning of the [local order] that falls within the mayor's powers. No other arguments have been invoked by the mayor from which it appears that the term "public place" within the meaning of the [local order] could also include a group chat on social media. Therefore, the court does not follow the mayor's contention that a group chat on Telegram is a public place within the meaning of the [local order]."

mayors to impose online restraining orders in analogy with the physical world the current administrative measures are aimed at.

5. *Transposing 'physical' legislation to the online space*

Considering the above, online applicability of administrative measures touches upon an interesting discussion, namely to what extent legislation applicable to physical places can be transposed to online spaces. More specifically, it questions to what extent administrative bodies have competency over privately-owned online spaces when the legislation their powers are based on solely foresees 'physical-space' interference. Therefore, a comparison of similarities and discrepancies between these two types of spaces can serve to answer what an updated version of the Dutch Municipal Act should include to make sure that mayors have sufficient powers to maintain public order whilst simultaneously safeguarding freedom of expression on the Internet.

In the Belgian equivalent of the Dutch Municipal Act for the city of Brussels, online spaces have been explicitly included in the terminology of publicly accessible spaces:

"For the purposes of these regulations, the term "publicly accessible space" includes, in addition to real spaces, virtual spaces accessible to the public, such as accounts on social media, forums and other digital platforms that are not limited to a small number of individuals who share common interests."[25]

The Brussels municipal act explicitly expands the competences of the public administration to a very broad interpretation of 'virtual spaces'. However, the answer to whether physical and online spaces overlap or are interchangeable is not as easy as portrayed by the Belgian regulation. The online space is not easily caught in a definition, and the Belgian example seems to demonstrate this perfectly. One could for example debate whether 'social media accounts' are 'virtual spaces accessible to the public'. In general, users can pick who to show their social media account, which renders it per definition not publicly accessible. Similarly, the limitations to exclude 'individuals who share common interests' and the terminology of 'a small number of individuals' are too vague to apply online. One could argue that anyone with a Telegram account has a common interest (to send messages). Similar argumentation would apply to online forums such as Reddit (discussing topics), or data platforms like Instagram or TikTok (entertainment).

The discussion on whether legislation from the physical world can be transferred to the online world is not new and is neither confined to the borders of administrative law. Platforms connect their users in a scale that has hitherto not been seen and have (at least partially) taken over the role of the state in safeguarding communicative spaces.[26] Due to the control data platforms have over the behaviour of users on their service, and consequently, over their users' communication possibilities in general, scholars have argued to regulate the access to and content on these platforms from various angles.[27] The same discussion – do platforms constitute *public places*? – must be tackled when looking at the application of administrative measures. Even though the specific administrative measures in article 172a were written with physical territorial borders in mind, the main requirement for a mayor to act depends on whether the place is

[25] The *Gemeenschappelijk algemeen politiereglement voor alle 19 Brusselse gemeenten* (valid from 1 April 2020), article 1 §5 (translation from Dutch by the author), available at: www.brussel.be/sites/default/files/bxl/Reglement_de_police_-_Politiereglement.pdf (accessed 30 November 2022).

[26] S. Benesch, *But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies*, in *Yale Journal on Regulation*, 2020, www.yalejreg.com/bulletin/but-facebooks-not-a-country-how-to-interpret-human-rights-law-for-social-media-companies accessed 13 September 2021; N. Helberger, J. Pierson and T. Poell, *Governing Online Platforms: From Contested to Cooperative Responsibility*, 34 The Information Society vol. 34, n. 1, 2018, 1.

[27] Whilst some argue to stick closely to the private nature of data platforms, others argue that data platforms provide a public communicative sphere where ideas and information are exchanged, see J. Burkell and others, *Facebook: Public Space, or Private Space?*, in *Information, Communication & Society* 2014, 974; A. Bruns and T. Highfield, *Is Habermas on Twitter?: Social Media and the Public Sphere*, in A. Bruns, G. Enli, E. Skogerbo, A. Larsson, C. Christensen (eds.) *The Routledge companion to social media and politics*, New York & London, Routledge, 2016, 56; M.S. Schäfer, *Digital Public Sphere, The International Encyclopedia of Political Communication*, in *The International Encyclopedia of Political Communication*, 2016; A.P. Heldt, *Merging the "Social" and the "Public": How Data platforms Could Be a New Public Forum*, in *Mitchell Hamline Law Review*, vol. 46, issue 5, 1; P.L. Morris and S.H. Sarapin, *You Can't Block Me: When Social Media Spaces Are Public Forums*, in *First Amendment Studies* vol. 54, No. 2020, 52.

publicly accessible. A mayor can solely exert the powers in the Municipal Act in public places or places that are accessible to the general public.

From this starting point, an application of the rules to online spaces by analogy might prove a suitable solution.[28] *Public* does not necessarily equal *not privately owned*. Privately-owned property can also be publicly accessible, but that is not the case for all private property.[29] To make a proper analogy, the differences in the physical and online world must be considered. It is here that the disparities in the two types of infrastructures become evident. In the physical world 'access is allowed unless it is explicitly restricted'.[30] One can enter a physical place, until the proprietor decides to build a fence, lock the entrance, or take other measures to obstruct access. In that sense, deciding whether a physical place is publicly accessible depends solely on *accessibility*.[31] The online space does not function in that way. The technical interface of data platforms does not allow a user to join the platform without accepting its terms of service. As such, there is no default accessibility. In the online space, all access is restricted, unless it is explicitly allowed – except for a few open platforms.[32] That is exactly opposite from the structure in the physical world.

That does not mean that an analogy cannot be made. In the physical space there are places that function similarly to data platforms. One can access these physical places, but to do so, one must accept the house rules.[33] Rather than focusing on accessibility, an interesting parallel can be drawn when considering the Dutch case-law on these types of physical places and compare them to the aim of users when using data platforms.

In various occasions, Dutch courts have ruled that certain types of private companies are not at liberty to define their house rules or to (arbitrarily) refuse access to their physical property. This is the case if the property is (i) publicly accessible and (ii) used to fulfil a 'societal role' (*maatschappelijke functie*). Examples consist of a football stadium,[34] a nursing home,[35] and a house of worship.[36] Interestingly, an underlying, identical line of thought links together these types of properties and as such the limitations to the liberty to exclude visitors. None of these places are visited for the characteristics of the property itself, nor are any of them a one-of-a-kind place – there are other football stadiums, nursing homes, and houses of worship that can be visited instead of the specific property. However, when one visits a football stadium, one visits this exact property to cheer for the team playing on the field. Similarly, one visits a certain nursing home because a relative is being taken care of in said property, just as one visits a house of worship due to the connection with the (religious) group connected to that certain property. As such, these places become a one-of-a-kind-property due to visitors' *aim of visiting*. Another football stadium, nursing home, or house of worship would simply not be a sufficient alternative to the exact property. Online users of data platforms decide to sign-up for an online platform in a similar way as people decide to visit specific types of property. A user signs up for a specific platform, because friends, family, or other likeminded groups are present on the platform, or because there is

[28] See on this analogy: W. Bantema and others, *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*, in www.politieenwetenschap.nl/publicatie/politiewetenschap/2018/burgemeesters-in-cyberspace-313 accessed 28 November 2022, 29 ff.

[29] See for an example the case of *Appleby*, where the right to publicly protest and freedom of expression were at stake in a privately-owned, but publicly-accessible shopping mall: *Appl. No. 44306/98 (Appleby and Others/United Kingdom)* (2003) ECLI:CE:ECHR:2003:0506JUD004430698 (ECtHR).

[30] See further on this also B. van der Donk, *Digital Bouncers. A European roadmap to navigate access rights and moderation issues on social media platforms*, PhD Thesis, Copenhagen, University of Copenhagen, 2023, 123-125.

[31] It has been argued that 'accessibility' can also be used to define whether online spaces are public, but I strongly disagree with this. See for the discussion: Bantema and others (n 22), 29, discussing the work of Vols (2010) on using accessibility as a requirement to decide whether physical and online places are publicly accessible.

[32] Such open platforms (a platform that does not require a sign-up before entering and does not apply implicit user terms) are extremely rare in the current age of the Internet. To date, one of the only platforms providing such an open service is Chatroulette (chatroulette.com).

[33] B. van der Donk, *European views on the privatization of the "online public space"*, 29 June 2022, Media Research Blog, https://leibniz-hbi.de/de/blog/european-views-on-the-privatization-of-the-online-public-space (accessed 1 December 2022).

[34] *District Court Gelderland (Stadionverbod Vitesse)* (2015) ECLI:NL:RBGEL:2015:452, §4.2.

[35] *Appeals Court Arnhem-Leeuwarden (Nursing home)* (2013) ECLI:NL:GHARL:2013:6873, §4.7.

[36] *District Court 's-Hertogenbosch (Refusal of entry to a mosque)* (2009) ECLI:NL:RBSHE:2009:BH4029.

specific information or content to be found. There is a specific *aim of visiting*, which cannot be substituted by joining another platform (yet[37]).

By analogy, that means that data platforms that are publicly accessible - meaning not aimed at or (technically) limited to a specific group of persons – and which fulfil a societal role, should adhere to a duty of care to safeguard public access to their service. Similarly, as the competences of mayors apply to physical places that are publicly available, it seems desirable that at least the spaces that fall within the definition of publicly accessible and societal relevant fall within the scope of power of mayors. This extra requirement would simultaneously balance the interests of the platform (right to property and the freedom to conduct a business) and guarantee that the administrative measure does not interfere in a disproportionate way with the users' right to private life and freedom of expression.

6. *Concluding remarks: the future of online restraining orders*

That brings us to the concluding remarks of this article. The first online restraining order in the Netherlands that was issued in November 2021 was based on an unstable legal foundation. The Dutch Municipal Act imposes powers on a mayor to safeguard the public order in the municipality. These powers, however, were intended to have effect in the physical world only, as reflected by the wording of the provisions in article 172a. Stretching these provisions - in their current form - to also include the online world, would jeopardize the principle of legality.

Following the public intentions of the mayors of Amsterdam, Rotterdam, and the Hague to experiment with online restraining orders, and the imposition of the first online restraining order in Utrecht, there is a clear call from practice to provide legislative options to tackle online disruptive behaviour. The preventive nature of administrative measures proves a good basis for curbing online content that can lead to harm in the physical world.

As such, there is a need for a legislative update. The Belgian inclusion of 'virtual spaces' in Brussel's Municipal act is an example of such a legislative update. However, an updated Dutch version should preferably not be worded similarly to its Belgian counterpart. The latter's terminology does not provide a sufficient future-proof basis for administrative measures, and it does not strike a sufficient analogy between physical properties included in the administrative competences and privatelyowned properties in the online world. The sole requirement of 'accessibility to the public' does not work adequately in the online world, due to the technical infrastructure applied by platform services. This leads to legal uncertainty. Rather than sole accessibility, the power to impose administrative measures should also be limited to those places that fulfil a service with a societal interest. These are places (whether online or physical) that due to their aim of visiting constitute a unique place – an aim that cannot be substituted by offering access to another platform or property. This terminology allows for a future-proof system, where any potential changes in the Internet infrastructure can be addressed on a case-by-case assessment.

Lastly, since data platforms are an important source of information and way of communication, the law will have to reflect the same safeguards that it prescribes for physical restraining orders when imposing online administrative measures. This to ensure that freedom of expression is not unduly restricted. That means that administrative measure must comply with the provisions on the maximum-time duration, and the necessity and proportionality requirements. Since Dutch mayors can only impose administrative measures within their own municipality, online restriction orders must reflect this. As such, as was the case in the online restraining order imposed by Dijksma, the measure must be limited to content that affects a specific municipality and may under no circumstances result in a full-access restriction to the Internet.

[37] Platform interoperability might be able to solve the problem created by exclusivity. If users of one platform can reach users on another platform, there is no longer a need to be a member of a certain data platform. Whether this can adequately solve the problem will be proven in the next years, as the newly adopted Digital Markets Act (Regulation (EU) 2022/1925) stipulates interoperability obligations for (certain) gatekeepers of communications services in article 7.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 161-170
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 13

*Data Processing in Public Health: The Role of Information Systems**

Luigi Rufo
(Research Fellow at University of Padova)

ABSTRACT This paper addresses the topic of information systems in public health and issues related to the protection of personal data. In particular, a number of information systems found in Italian public health care will be analyzed: for example, the electronic health record, the electronic medical record, and the health file. It will also address the principle of privacy by default and by design and its proper application to properly design a modern information system.

1. *Introduction*

New technologies and the increasing use of digitization in diagnostic and therapeutic pathways are radically changing medical practice.[1] In addition to offering new opportunities for access and continuity of care, these innovations help strengthen prevention, improve quality of life and increase its expectancy. Indeed, current public healthcare is increasingly and boldly trying to rely on new technologies to improve habits, lifestyles, circular methods of communication and information-sharing between doctors and patients.[2]

Smartphones, wearable devices, and social networks have become an appendage of the human body: an "extended body"[3] endowed with evolutionary autonomy and consisting of intangible streams of information that can be processed and exchanged among multiple parties, even geographically distant.

The Covid-19 pandemic has also made evident to the whole world the central role played by digital technologies, which in the field of health protection will have to support the various national governments in meeting the challenge of sustainability and prevention by taking high quality, accurate, informed, and above all quick decisions.

Today, data both in raw and aggregated form represent the "new oil"[4] in public-health policies, as well as the cornerstone of the continuous development towards IoT and artificial-intelligence systems, - tools that may be a central part of any future decision-making, posing the additional challenge of how to improve the ability to "read" and exploit data.

In this framework of continuous development, the digitization and sharing of health data would thus enable a data-driven[5] approach by professionals working in public-health facilities, thus creating not only diagnostic and therapeutic pathways that are more adherent to the needs of patients-especially for those affected by chronic diseases-but also promptly leading to the conclusion of projects related to the study of diseases, as well as research and development of new treatments.

However, in order to outline not only a national and/or regional but also a territorial strategy on improving the use of data, it will be necessary to focus attention toward several unavoidable points of observation, leveraging on both currently available information-technology standards and collaboration among the various public-health players.

Indeed, first of all it will be necessary to

* Article submitted to double blind peer review.

[1] T. Schael, *Sanità elettronica e servizi digitali al cittadino. La rivoluzione delle ricette e dei certificati di malattia*, in *eHealthcare*, n. 3, 2009, 13.

[2] See A.D. Weston and L. Hood, *Systems biology, proteomics, and the future of health care: toward predictive, preventative, and personalized medicine*, in *Journal of Proteome Research*, n. 3, 2004, 179-196; P. Cappelletti, *La Medicina Personalizzata fra ricerca e pratica clinica: il ruolo della Medicina di Laboratorio*, RIMeL/IJLaM, 2009, n. 5 (Suppl.), 26-32; Q. Tian and Others, *Systems cancer medicine: towards realization of predictive, preventive, personalized and participatory (P4) medicine*, in *Journal of Internal Medicine*, n. 271, 2012, 111-121.

[3] M. Mancarella, *eHealth e diritti. L'apporto dell'Informatica giuridica*, Rome, Carocci, 2014, 15.

[4] A. Charles, *Tech giants may be huge, but nothing matches big data*, in *The Guardian*, 2013.

[5] See Z. Hou and Z. Wang, *From model-based control to data-driven control: Survey, classification and perspective,* in *Information Sciences*, 2013, 3-35; S.L. Brunton and J.N. Kutz, *Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*, Cambridge, Cambridge University Press, 2017, 414- 416; V. Breschi, A. Chiuso and S. Formentin, *The role of regularization in data-driven predictive control*, in *arXiv preprint*, Singapore, 2022.

take into consideration the technologies and procedures already implemented by hospitals and local health trusts in order to avoid the use of obsolete models or tools. Then it will be necessary to consider, step by step, the current technological framework with the aim of reaching possible and complete interoperability of information systems and public databases.

Undoubtedly, in Italy several tools, each according to its level of use, play a key role in the management of data related to citizens' health: Electronic Health Record (so-called Fascicolo Sanitario Elettronico - FSE), which is of regional level, Health File (so-called Dossier sanitario elettronico - DSE), and Electronic Medical Records (so-called Cartella clinica elettronica - CCE) specifically linked to health facilities.

Such information systems, through their application potentials in part still unexplored, are key strength in the public-health sector being based on the centrality of patients and sharing and management of their clinical information. They allow to promote self-determination (so-called "patient empowerment"[6]), which implies a process of personal development in which patients, in a partnership relationship with health professionals, are provided with knowledge, skills, and greater awareness of health treatments. In other words, an information flow that is not uni-directional but bi-directional or, even more precisely, circular can be developed.[7]

With regard to this issue, Italian law makers - in four first historical stages - i) Decree Law No. 158 of September 13, 2012; ii) Decree Law No. 179 of October 18, 2012 which provided, in Section IV, Art. 12 the FSE and Surveillance Systems in the Health Sector - and Art. 13 - Medical Prescription and Medical Records; iii) Decree "Fare" approved in June 2013; iv) Presidential Decree of September 29, 2015 no. 17, which defined the rules by which the Regions must set up their own FSE systems - was designed to adopt measures aimed at concretely introducing into the national law tools that, besides improving efficiency, effectiveness and appropriateness of care, help patients keep their data and information up-to-date in their own health records, managed in total autonomy and self-determination.[8]

In this frame of reference, it is also interesting to take into account the provision of the Italian Data Protection Authority ("Privacy Authority") which, when called upon to express an opinion on the DSE, defined it as one of the "numerous initiatives under way to improve the efficiency of the health service by a further development of networks and more extensive IT and telematic management of acts, documents and procedures".[9]

We can thus argue that clear, reliable and up-to-date data and information are a strategic asset to enable public healthcare providers to optimize their care processes and provide their patients with increasingly better services while also avoiding errors.

2. *Information systems in public health: from the electronic medical records to electronic health record*

An information system can be technically defined as a set of interconnected elements that collect (or search), process, store and distribute information to support decision-making and control activities in healthcare organizations.[10]

Before the introduction of electronic tools,

[6] R.M. Anderson and M.M. Funnell, *Patient empowerment: reflections on the challenge of fostering the adoption of a new paradigm*, Patient Education and Counseling, 2005, 153-157; L. Buccoliero, *E-HEALTH 2.0 - Tecnologie per il patient empowerment*, in *Mondo digitale*, 2010; G. Ferrando, *Diritto alla salute e autodeterminazione, tra diritto europeo e costituzione, in Politica del diritto*, XLIII, 1, 2012; L. Rufo, *Profili giuridici del Personal Health Record: tra diritto all'autodeterminazione e tutela della privacy*, in C. Faralli, R. Brighi and M. Martoni (eds.), *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth*, Turin, Giappichelli, 2015, 321-333.

[7] L. Rufo, *Il Dossier sanitario elettronico. Un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito clinico*, Bologna, Il Mulino, 2018, 4.

[8] See M.G. Virone, *Il Fascicolo Sanitario Elettronico. Sfide e bilanciamenti fra Semantic Web e diritto alla protezione dei dati personali*, Rome, Aracne, 2015, 145.

[9] Garante Privacy, *Registro dei provvedimenti n. 331 - 4 June 2015*, [doc. web n. 4084632].

[10] K. Laudon, *Management dei sistemi informativi*, Milan, Pearson, 2006, p. 17-19; N. Agabiti, M. Davoli, D. Fusco, M. Stafoggia and C. A. Perucci, *Valutazione di esito degli interventi sanitari*, in *Epidemiologia & Prevenzione*, Milan, Inferenze, 2011, n. 35, 1-80; C. Caccia, *Management dei sistemi informativi in sanità*, Milan, McGraw-Hill, 2008; C. Caccia and G. Nasi, *Il sistema informativo automatizzato nelle aziende sanitarie*, Milan, McGraw-Hill, 2002; L. Buccoliero, C. Caccia and G. Nasi, *e-He@lt: percorsi di implementazione dei sistemi informativi in sanità*, Milan, McGraw-Hill, 2005; A. Teti and G. Festa, *Sistemi informativi per la sanità*, Milan, Apogeo, 2009.

information management took place on paper, thus requiring the work of recording, storing documents and searching for them, with consequent limitations from the point of view of efficiency. The advent of information and communication technologies (ICT) has significantly improved the situation. Data can already be *ab origine* provided with the meaningful "form", which being useful to get information, results in improved health-care services to protect both individual and community health.

The essential elements shaping an information system are: data (essential component of the system and initially not yet processed); information (set of processed data); people (the recipients of the processed information); tools (the set of equipment capable of transferring information from one subject to another); and the processes (set of criteria that allow to understand the way in which data is collected and processed).

However, depending on the state of computerization of care processes, various strategies and models for organizing clinical data can be envisaged.

Among the systems of electronic recording/archiving of patient clinical data used in public-health care, the following are in place: the Electronic Medical Record (so-called CCE); Health File (so-called DSE) and the Electronic Health Record (so-called FSE).

The model best known so far in the national and international context is precisely the so-called Electronic Health Record, which is characterized by its organizational structure built on a unified corporate clinical "data repository". In such a repository, all health information produced in the various therapeutic processes, which see the patient as a primary actor, is brought together and is accessed by the several health professionals working in the facility.

Thus, there has been a shift in recent decades from the design of healthcare institution "episode records" (Electronic Medical Record) to the creation of healthcare institution "system records" (Electronic Health Record), which can offer a longitudinal view of patient health. This model collects and stores clinical data and information of patient pathways in a Data Base (DB).[11]

2.1. *Electronic medical records*

The medical record constitutes the official and legally-recognized document for the systematic and functional collection of data on a patient's medical history within a public hospital. In the European sphere, the European Commission's Recommendation of July 2, 2008 on cross-border interoperability of electronic medical records systems, under Article 3(c), defines CCE as: "a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes".[12]

At the national level, though there is no precise definition, doctrine and jurisprudence agree that the CCE is "a public document having the function of a diary of medical intervention and the relevant clinical facts so that the facts must be recorded in accordance with their occurrence".[13]

The above is also reflected in Article 26 of the new Code of Medical Ethics, which provides that "The medical record of public and private health providers must be drawn up clearly, with punctuality and diligence, in compliance with the rules of good clinical practice and contain, in addition to any objective data related to the pathological condition and its course, the diagnostic-therapeutic activities provided. The medical record must record the manner and timing of information as well as the terms of consent of

[11] Collection of data managed through a Data Base Management System (DBMS). The data are structured and linked together, at the logical level, in accordance with the representation model (e.g. relational) adopted by the DBMS and, at the physical level, reside on memory devices organized in particular structures. Users interface with the database through a Query Language (e.g. SQL). For more information: P. Atzeni, S. Ceri, S. Paraboschi and R. Torlone, *Basi di Dati: modelli e linguaggi di interrogazione,* McGraw-Hill, Milan, 2013; R. Ramakrishnan, *Database Management Systems*, McGraw-Hill / Asia, 2004; R.A. Elmasri and S.B. Navathe. *Sistemi di basi di dati Fondamenti,* Addison Wesley, 2004.

[12] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (2008/594/CE).

[13] B. Primicerio, *La cartella clinica e la documentazione sanitaria ad essa collegata: evoluzione, utilizzazione e responsabilità*, in *Il Diritto sanitario moderno*, 2004, 207; V. Vaccaro, *La cartella clinica*, in *Trib. amm. reg*., 2003, 180; G. Rocchietti, *La documentazione clinica. Compilazione, conservazione, archiviazione, gestione e suo rilascio da parte della direzione sanitaria. Trattamento dei dati sanitari e privacy*, in *Minerva medicolegale*, 2001, issue 1, 15; O. Bucci, *La cartella clinica. Profili strumentali, gestionali, giuridici ed archivistici*, Santarcangelo di Romagna, Maggioli, 1999.

the patient - or his or her guardian - to diagnostic and therapeutic proposals; it must also record the patient's consent to the processing of sensitive data, with particular regard to cases of enrollment in an experimental protocol".

In light of this, computerization of the medical record, with a view to making health-care processes more efficient, flexible and responsive to people's needs, is part of a broad context of internal reorganization in hospital facilities, also enabling the introduction of important improvements in data management, complying with the requirements of completeness and integrity.

However, over time, the CCE has been seen as a mere evolution of the Paper Medical Record (so-called Cartella clinica cartacea - CCC); but it should be noted, instead, that it represents one of the most accurate tools of eHealth for systemic and structured management of data referring to the clinical history of patients in in-patient or out-patient settings by promoting the continuity of patient care in the same health facility through the sharing and retrieval of clinical data recorded.

The added value of the CCE with respect to the CCC is well outlined in a textual passage of the Guidelines of the Lombardy Region, in the following terms: "The CCE is therefore configured as an integrated corporate IT system, to be understood as a transversal tool for the various care processes, replacing the paper medical record, which on the one hand meets the requirements and functions of the latter, and on the other hand solves some critical issues related to it, offering opportunities to increase the value through integration with other IT tools. It is important to recognize the electronic tool as having its own dignity, which also determines a strong difference in the way it fulfills its functions compared to the paper tool. The electronic tool today is capable of fulfilling all the tasks formally defined for the paper medical record, but it is necessary and desirable that it does so differently, that is, according to the logic of effective and efficient electronic data management. For this reason, the concept of the electronic medical record tool as the mere "digitizer" of paper, to be implemented without an adequate review of internal processes, is reductive-if not erroneous-and does not allow the potential in terms of integrated information management, timeliness, automation, and simplification offered by the ergonomics of the digital tool to be exploited".[14]

Typically, a CCE consists of several functional blocks such as administrative documentation; informed consent; initial medical and nursing clinical framing; clinical management (vital-parameter documentation, invasive-procedure documentation, nursing-care sheets, medical reports, etc.); medication-therapy management (often delegated to an external, enterprise-integrated application); and transfer and discharge documentation.

Another relevant element, referred to in the privacy regulations, is that appropriate safeguards must be established with respect to access to data by health professionals, patients and third parties, with regard to measures of a technical nature such as identification, authentication and authorization of the individuals who will have access to the system. An additional aspect, which is very important for privacy, is the need to separate the different categories of data that may be included in the electronic medical record, providing a modular structure to be aligned with the various purposes of processing and/or the individuals who may access the data.

Lastly, an important aspect that should not be overlooked concerns the rules on the processing of personal data which give primary importance to the principle of self-determination on the use of the Electronic Health Record, which leads to the obligation to plan appropriate moments for informing patients to express true consent (opt-in) or forms of dissent (opt-out).

It should be noted that the Italian Data Protection Authority, called upon to express an opinion on the mechanisms that a CCE system must implement, has stated that "in addition to compliance with privacy regulations, IT security requirements must also to be met, which may vary in relation to the use that is made of the data and with respect to possible data transfers to third countries".[15]

2.2. *Health file*

As early as 2009, although in the - still persisting - absence of a legal definition at the national level, the Privacy Authority felt the

[14] Regione Lombardia, *Linee guida per la Cartella Clinica Elettronica Aziendale*, v. 02.1, 2012.
[15] Garante Privacy, *Registro dei provvedimenti n. 131 - 15 February 2007,* [doc. web n. 1607201].

need to determine specific guarantees, responsibilities and rights with reference to the Electronic Health Record. Against this background, the Authority adopted the Guidelines on Electronic Health Record and Health File.

Specifically, these Guidelines defined the electronic health record as "the tool established at a health-care organization as a single data controller (e.g., hospital, health trust, nursing home) within which several professionals operate, through which information is made accessible, inherent to the health status of an individual, relating to present and past clinical events (e.g., laboratory reports, documentation relating to hospitalizations, emergency department access), aimed at documenting the clinical history".[16] In other words, the health file was intended as a collection of present and past clinical events related to an individual patient and processed exclusively at a single health facility, with a view to documenting patients' entire clinical history.

However, the significant increase in the use of this information system for the management of health records in public facilities on the one hand and, on the other, the results of inspections which caused many sanctions led the Privacy Authority in 2015 to provide new and specific Guidelines on the Health File.[17]

By this way, also thanks to the Privacy Authority, as of today DSE can be appropriately framed as a digital tool related to eHealth whereby it is possible not only to store the patient's entire medical history with reference to the services provided within a given health facility, but also to keep track of the diagnostic, therapeutic and care pathway throughout patients' lifetime.[18]

The usefulness of DSE is undeniable: just think of the examination results-sometimes invasive and not repeatable in the short term-already carried out on the person concerned and to which the doctor will be able to have access, without necessarily having to repeat the same, with enormous savings of both time and money; or, again, think of the advantage deriving from the implementation of this tool with reference to subjects suffering from chronic pathologies, of which the doctor will thus be able to become immediately aware by adopting all due precautions aimed at reducing and/or eliminating the risk of error in the administration of specific health treatments.

However, as also pointed out by the Privacy Authority, in order for the health files to be effective in the diagnosis and treatment of patients, it is necessary that they be created in such a way as to ensure the certainty of the origin and correctness of the data, as well as the accessibility of the same only by legally-entitled persons. As a consequence, the Privacy Authority considered the creation of this tool optional, which implies that, in the absence of an explicit self-determination of the interested party to the creation of the same, it would be impossible to open a file as DSE. In any case, failure to consent to the establishment of DSE cannot in any way affect access to medical care, which is a right enshrined in the Italian Constitution. On the contrary, in case of consent to the creation of DSE and entering data, the purposes to be pursued must be exclusively linked, as a guarantee for patients, to the prevention, diagnosis, treatment and rehabilitation of the person concerned, without further possible uses.

However, the Privacy Authority has actually decided it is possible to pursue administrative purposes (e.g., booking through the CUP or payment for a health service) through DSE, but it must be structured in such a way that the administrative data is separated from the health data and that different enabling profiles are provided for the individuals who have access to the DSE, due to the function of the operations they can perform.

A further major element is the need to make sure that the person concerned be able to decide to obscure certain health data or documents, which will therefore not be visible and consultable through Dossier sanitario elettronico by health professionals who access it; or else, detailed access "enabled" from time to time by the patient should be provided for.

2.3. *Electronic health record*

The Electronic Health Record, provided for in Article 12, Decree Law No. 179 of October 18, 2012 concerning "Further Urgent

[16] Garante Privacy, *Linee guida in tema di Fascicolo sanitario elettronico e dossier sanitario,* [doc. web n. 1598313].
[17] G.U. n. 164 of 17 July 2015, more information: www.gpdp.it, [doc. web 4084632].
[18] L. Rufo, *Il Dossier sanitario elettronico. Un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito clinico*, 25.

Measures for the Country's Growth," is a tool whereby citizens can track and consult their entire-life health history, sharing it with health professionals to guarantee a more effective and efficient service.

All the information and documents that make up FSE are made interoperable to allow it to be consulted and populated throughout the country, not just in the patient's region of residence. This offers patients greater freedom in choosing care and sharing information, all of which is available through access to FSE by health-care professionals.[19]

In addition, access to FSE by health professionals, especially in emergency situations, allows them to know everything they need to intervene promptly and guarantee the health outcome. In other words, in the FSE system, the patient is at the center of the system with his/her health history and every medical action concerning him or her tracked and codified, also avoiding the repetition of unnecessary clinical investigations. All this is done in compliance with the conditions defined by the persons themselves at the time of the first access to FSE and such conditions can be changed at any time. Patients, in fact, can choose who is authorized to consult their FSE, under what conditions and also what data, choosing, therefore, also to obscure some information. In addition, they can view who accessed FSE and when.

FSE is therefore defined in the national legislation as the set of health and social-health data and digital documents generated by present and past clinical events concerning the patient, and has as its main objectives: to facilitate patient care; to offer a service that can facilitate the integration of different professional skills; and to provide a robust information base.[20]

The FSE also pertains to a wide range of activities, regulated by the Ministry of Health, related to the delivery of health services. Specifically, it is aimed at the overall improvement of the quality of services concerning: prevention, diagnosis, treatment and rehabilitation; study and scientific research in the medical, biomedical and epidemiological fields; health care planning, checking of the quality of care and evaluation of public-health care.

In this regard, it is interesting to make some comments on the implementation and utilization of indicators of FSE, which has had a strong implementation momentum with the Covid-19 pandemic.

Specifically, the implementation indicators aim to represent the state of progress about the implementation of the regional FSE, whereas the utilization indicators are aimed at monitoring the actual level of use and diffusion of the FSE throughout the country by citizens, physicians and health-care providers. On the implementation side, we must note that, out of twenty regions, as many as fifteen regions have reached 100% of the implementation outcome, four of them have reached 90%, and fortunately only two regions scored 80%.

On the other hand, looking at the indicators of utilization, there are significant differences among the several actors analysed. In particular, a general backwardness emerges in the use of FSE by physicians and by citizens. Better data is found for use by Health Authorities, although in several regions data is close to zero.[21]

It is undeniable that from the current scenario of FSE implementation, a partial use of the same emerges compared to its use as a support for patient care. In fact, FSE should be viewed as a true decision-making tool capable of collecting and making available the entire medical history of a patient.

This is especially true in the long run since, at the research level, FSE could lead toward the creation of a national health repository that may ensure the use of data for health research and be a key source of information.

On the side of data-protection regulation, it should be noted that during the pandemic period an important innovation was introduced. Indeed, in order to accelerate the activation and use of the FSE by all patients, Article 11 of Decree Law No. 34 provided that, as of the date of publication of the decree, the activation and population of the FSE will take place automatically, with the elimination of the "consent to entering" so that

[19] P. Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, Trent, University of Trent, 2011; L. Califano, *Fascicolo sanitario elettronico (Fse) e dossier sanitario: il contributo del Garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in *Sanità pubblica e privata*, Santarcangelo di Romagna, Maggioli, issue 3, 7-22, 2015.

[20] M. Moruzzi, *Il Fascicolo Sanitario Elettronico in Italia. La sanità ad alta comunicazione*, Milan, Il Sole 24 Ore, 2011.

[21] More information: www.fascicolosanitario.gov.it/

patients can easily consult their social-health documents, even if generated by public-health facilities located outside the region they come from, thanks to the interoperability ensured by the Health Insurance Card System. In addition to this, regardless of the consent of the patient, health-governing bodies can access pseudonymized data in FSE to carry out related institutional functions (e.g., care planning, health-emergency management).

Furthermore, on October 5, 2020, following this important regulatory change, the Privacy Authority issued a specific opinion regarding the process of populating FSE, with respect to the issue concerning the entering of data prior to May 2020, stating that, in order to guarantee the rights of data subjects, an adequate information campaign had to be carried out at the national and regional level aimed at: i) making data subjects aware of the characteristics of the processing carried out through FSE, with particular reference to the new features introduced by the applicable regulations; ii) ensuring that the data subject could exercise the right to object to populate FSE with health data generated by clinical events prior to May 19, 2020, within a predetermined period, not less than 30 days.

3. *Privacy in public health information systems*

The possibility, inherent in ICT technologies, to process significant amounts of data at high speed and often without capillary control, even going so far as to trace detailed profiles of data subjects, has produced a consequent acceleration also in regulating the right to protection of the personal sphere of individuals.

Hence, it seems appropriate to analyze the context and development of information systems and their application in the public-health sphere by considering the European Data Protection Regulation No. 679 of 2016, which constitutes the new primary source of reference for the protection of personal data of individuals.

This new law has introduced clearer rules and stricter criteria with the aim of ensuring greater assurance to the data subject with respect to data processing through new information society technologies and better regulatory harmonization and alignment in the European context.

Indeed, while on the one hand the development of computer systems for storing and organizing data has positively favored access to care and improvement in treatment pathways, on the other hand, however, it has generated new dangers in terms of reliability and security, leading to the introduction of more stringent custody obligations on the part of operators, also imposed by the existing data protection legislation.[22]

Thanks in part to the GDPR regulations, key principles for the proper processing of personal and health data through information systems have taken shape, and they are essentially: a) minimization of the collection, use, disclosure and storage of users' identifying data;[23] b) participation and active involvement of users, among other things, allowing the exercise of powers of control during the lifecycle of processed personal data; and c) enhanced security of information. These principles should then be summarized under the broader definition of privacy by design and privacy by default, which, after a laborious legislative process that began on January 25, 2012, resulted in Article 25 of the GDPR, headed "Data protection by design and protection by default".[24] Yet, it should be noted how this Article, while providing a cogent and innovative contribution compared to the past, largely recalls the intrinsic essence of the principle of necessity in data processing, already contained in Article 3 of the Italian Privacy Code and extensively described in the provisions of the Privacy Authority, which states: "*information systems and computer programs shall be configured reducing to a minimum the use of personal data and identification data, so as to exclude their processing when the purposes pursued in individual cases can be achieved by means of, respectively, anonymous data or appropriate modalities that allow the data subject to be identified only in case of necessity*".[25]

[22] A. Cavoukian, *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Toronto, Information and Privacy Commissioner of Ontario, 2009.

[23] R. D'Orazio, *Protezione dei dati by default e by design*, in Sica and D'Antonio e Riccio (eds.), *La nuova disciplina europea sulla privacy*, Milan, Giuffré, 2016, 79.

[24] More information: EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, ver. 2.0., 20 October 2020

[25] In order to clarify these concepts expressed in Article 25, it's necessary to read Recital 78 of the GDPR: "The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures

This is a precept that, anticipating by a few years the formalization of the broader concept of privacy by design and by default, entails an important consequence in the context of data processing carried out with automated systems. Indeed, according to the principle of necessity, information systems and computer programs must be configured to handle data anonymously-for example, through the use of an alphanumeric code-so that the data subject cannot be directly identified.[26]

However, particularly interesting for the purposes of the present analysis is to note how this concept is also in wide use in the field of digital health, with the peculiarity that its fulfillment in this sector is not relegated to the technological aspect of information-systems design and development alone, but also affects the phase of implementation and adaptation of the facilities' premises. Take, for example, server rooms or offices where there is a risk, through unauthorized access, of illicit disclosure of the sensitive data of the persons concerned.

What distinguishes the concept of privacy by design and privacy by default[27] are undoubtedly seven pivotal "elements": Proactive not reactive; Privacy as the default setting; Privacy embedded into design; Full functionality - positive-sum, not zero-sum; End-to-end security - full lifecycle protection; Visibility and transparency - keep it open; Respect for user privacy - keep it user-centric.[28]

3.1. *Proactive not reactive*

The first element of privacy by design is characterized by actions with a proactive rather than reactive approach. Indeed, it is much more useful to prevent and address critical issues before they turn into actual, active harm, so that promptness in acting, even before the problem may arise, is an added value in design and characterizes this principle by favoring the protection of information.

However, it is relevant to emphasize that the above is valid only if there is constant monitoring of the development project and willingness to set high standards of data protection and security.

In the public health sector, it is easy to believe that this principle is crucial: the prevention and anticipation of possible breaches of health data through abusive access to information systems makes it possible to achieve a perception of high reliability of healthcare facilities among patients, as well as to reduce/eliminate subsequent architectural interventions, thus saving additional costs for possible recovery.

3.2. *Privacy as the default setting*

Privacy by design through the default setting of an IT system seeks to achieve the highest level of personal-data protection. Based on this principle, the user will be able to rely on the setting built into the system to maintain his or her degree of privacy without having to take any action.

For users this is an important principle as they are the primary actors in the management of their own information.

The concepts on which privacy by default is based are privacy protective and data minimization.[29] The first concept concerns the

be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders".

[26] F. Bravo, *Data Management Tools and Privacy by Design and by Default*, in R. Senigaglia, C. Irti and A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Singapore, Springer, 2022, 85-95.

[27] F. Bravo, *L'architettura del trattamento e la sicurezza dei dati e dei sistemi*, in Cuffaro and D'Orazio and Ricciuto (eds.) *I dati personali nel diritto europeo*, Turin, Giappichelli, 2019, 823.

[28] A. Cavoukian, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Toronto, Information and Privacy Commissioner of Ontario, 2010, 12.

[29] Principle derived from Article 6 paragraph 1 (b) and (c) of Directive 95/46/EC and Article 4 paragraph 1 (b) and (c) of EC Regulation No. 45 of 2001 and provides that personal data must be *"collected for specified, explicit and legitimate purposes*" and must be "*adequate,*

view that the design of an IT system takes into account a specific and effective purpose that legitimizes the collection of data. The second, on the other hand, mandates that data be processed only where strictly necessary. This encourages the implementation of a true prevention mechanism, which in the health care field could be implemented, for example, by using pseudonyms to identify and/or de-identify patients or provide for the automatic hiding of reports uploaded to healthcare organizations' information systems.

3.3. *Privacy embedded into design*

This principle states the importance of considering data protection and its management as an essential component in the design of a system, but without diminishing the functionality of the system.[30]

In order to fully stick to this principle, it is necessary to pursue the continuous updating of good implementation practices, standards and regulatory acts, such as laws and regulations, also taking into account technological progress.

In healthcare, this is achievable through the updating of standards and Guidelines for supporting the development and implementation of IT systems.

3.4. *Full functionality-positive-sum, not zero-sum*

Privacy by design via the development of this principle points to a vision that aims to reconcile all the interests and objectives involved in the development of an IT system. In other words, what it aims to achieve is the demonstration that privacy and security can coexist without having to forcibly choose to protect one aspect whilst neglecting another. A turning point is the creation of non-invasive systems that maintain only the strictly-necessary information.

3.5. *End-to-end security - full lifecycle protection*

Security is a key concept, and without it no responsibility and no rights could be assigned. In fact, only with the application of security-related elements privacy by design can ensure the full lifecycle of information to the end.

In light of what has just been said, the most delicate role is played by developers and designers, whose task is to apply security methodologies in order to eliminate, or at least reduce, not only the risk of theft but also the complete or partial deletion of data.

3.6. *Visibility and transparency*

Privacy by design seeks to ensure transparency to all stakeholders. The principle of transparency requires that information intended for the public or data subject be concise, easily accessible and easy to understand, and that plain and clear language be used. This principle is a relevant feature and leads to the concept of accountability. In other words, the data controller is required to demonstrate that the processing, through privacy policies, has been carried out in accordance with data-protection regulations.[31]

3.7. *Respect for user privacy - keep it user-centric*

As a first step, privacy by design requires designers and developers to give priority to users' requests and interests.[32] This way, the concept of "user-centricity" takes on two different meanings: the first, as the user's right to exercise control over his/her own information; the second, in terms of a factor that forges a system around the figure of the user, and thus around his/her needs. It follows that if users are recognized to have a way to manage information about themselves quickly and easily, the system will have to enable this outcome.

In healthcare, it is now a well-established fact that, via consent to medical treatments, the patient can almost totally self-determine his/her choices and be the focus of healthcare services; in the area of consent to data processing, the same approach should operate.

relevant and not excessive in relation to the purposes for which they are collected and/or subsequently processed."

[30] U. Pagallo, *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law*, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Cham, Springer, 2012.

[31] G. Finocchiaro, *L'accountability nel regolamento europeo,* in Barba e Pagliantini (eds.), *Delle persone. Commentario del Codice civile*, Vol. II, Milan, Giuffrè, 2019.

[32] R. Brighi e M.G. Virone, *Una tutela "by design" del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica,* in *A Matter of Design: Making Society trough Science and Technology*, Milan, Open Access Digital Publication by STS Italia Publishing, 2014.

4. *Conclusions and future perspectives*

IT, process innovation, person-centeredness and privacy are undoubtedly the four main drivers that are directing and changing "2.0" healthcare services within public health organizations, with tangible outcomes of improved patient management and clinical-risk prevention.

In addition, it should be added that the European Commission in February 2020 drafted a European data strategy, which is considered a central element of the technological transformation so much desired in the European NextGenerationEU program.[33]

That strategy has included healthcare among other areas, which was deemed "essential for making progress in the prevention, detection and treatment of diseases, as well as for making informed and evidence-based decisions to improve the accessibility, effectiveness and sustainability of health care systems"[34].

But there is more. Indeed, a corollary to the goal of this strong proactive boost of the European Commission is to ensure a reduction in health costs through better access, use and reuse of health data, with the long-term vision of redistributing resources by reprogramming ah essential levels of care.[35]

In this framework, the information systems of public healthcare organizations will play a key role since all clinical data produced by electronic health-record systems, medical devices and artificial-intelligence systems will be able to lead to their reuse also and especially for research and innovation (so-called secondary use of data).[36]

As also stated by the president of the Privacy Authority Prof. Pasquale Stanzione, "the digitization of healthcare is, in this sense, an extraordinary opportunity for development, innovation, competitiveness, to be promoted for the efficiency and universality of care and for better planning of healthcare expenditure. However, digital health must be realized within an organic and far-sighted project of health governance, which minimizes cyber risks and promotes selective data sharing, for the purpose of promoting research, but with due caution to avoid any possible re-identification of data subjects".[37]

In this framework with still uncertain contours, abidance by privacy legislation and its guiding principles may well represent the crux around which "expert" information systems can be developed. Sharing data in a European health-data space will make it possible to give more value to health not only as a fundamental right of individuals but also in the interest of the community in order to find immediate answers to common situations in the context of public health, as happened in relation to the Covid-19 pandemic but obviously always by fulfilling the centrality of human persons and their dignity.

[33] Regulation (EU) 2021/241 of the European Parliament and the Council 12 February 2021 establishing the Recovery and Resilience Facility.

[34] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, COM(2022) 197/2 final.

[35] V. Di Felice, *Lo spazio europeo dei dati sanitari*, in *Nota su atti dell'Unione europea*, Servizi studi del Senato, n. 102, July 2022.

[36] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020.

[37] More information: Garante Privacy, *Sicurezza del dato sanitario e condivisione* [doc. web n. 9747071].

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 171-184
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 14

*GDPR and Blockchain Technology in the New Multifaceted Scenario of Health Data Protection: Overcoming the Tensions Between Technology and Law**

Rolando Poggi
(PhD Candidate in Labour, Development and Innovation at University of Modena and Reggio Emilia and Member of Marco Biagi Foundation's Privacy Observatory)

ABSTRACT The EU General Data Protection Regulation n. 679/2016 (GDPR) stands as an element of support for the development of the digital economy. Among the many facets of society and areas of the economy that it influences, the GDPR also impacts on scientific research that uses personal data. The paper addresses the most important aspects of the GDPR that are relevant for the purposes of data protection in health research. Then, the study leverages the points of contrast between the "train of innovation" on which the new Distributed Ledger Technologies (DLTs; of which blockchain is the most celebrated example) travel at full speed and the rules contained in the GDPR. And indeed, despite the many tensions between the two actors (e.g., right to be forgotten, data controllership etc.) blockchain technology could be significantly propaedeutic for health research and for healthcare as a whole, and it could even reflect its advantages on the very culture of privacy regulation, by making data-protection mechanisms more efficient and by improving transparency in GDPR compliance paradigms. As a key to understanding, the paper uses one of the guiding principles of the GDPR: that of not hindering, but rather supporting technological progress. For this reason, blockchain will be deeply examined in its most relevant characteristics to investigate its extensive potential and, before that, its laborious compatibility with the legal requirements of the European regulation on privacy and with the main interpretative contributions from Europe's regulatory Authorities and Courts.

1. *Introduction: the complex scenario of privacy regulation in modern healthcare*

Data has become a milestone of economic and scientific development. In this context, data-protection legislation is constantly evolving: new contents and forms are emerging, and they require specific and diversified interventions by legislators. In *the broad horizons opened by new technologies, adequate measures are needed to protect personal data as well as a balanced regulation, capable of weighing opposing interests.

It is therefore essential to analyze in an interdisciplinary perspective the impact of the use and circulation of data and of disruptive emerging technologies on the main rules for data protection in human activities.

The implementation of the GDPR draws attention to issues that are important for the kind of scientific research that uses personal data. It was found that "an adequate analysis of health-related Big Data can help predict epidemics, treatments and diseases, as well as improve the quality of life and avoid preventable deaths".[1]

The need to manage patients' personal-health data correctly and appropriately has emerged with great evidence from the recent COVID-19 outbreak. The pandemic has confirmed (in a very harsh and urgent manner) that the use of patient data can be crucial for scientific research. In recent years, in the health sector (as in many other sectors) a considerable amount of data has been collected.[2] This aspect and the increase in the

*Article submitted to double blind peer review.

[1] "Proper analytics of big healthcare data can help predict epidemics, cures, and diseases, as well as improve quality of life and avoid preventable death", I.A.T. Hashem, V. Chang and N.B. Anuar, *The role of big data in smart city*, in *International Journal of Information Management (IJIM)*, vol. 36, 2016, 748; in this regard, see also A. Pentland, T. G. Reid and T. Heibeck, *Big Data and Health: Revolutionizing medicine and Public Health - Report of the Big Data and Health Working Group*, presented at World Innovation Summit for Health, Doha, 10-11 December 2013, 2.

[2] The availability of data will grow more and more, also as a result of new data sources such as sensors, social networks, mobile devices, (Internet of Things) being introduced into the social and economic spheres. E. Mor-

world population have led to new forms of health treatments and services.[3] And indeed, healthcare institutions currently experience an increased demand of real-world data from industry and research organizations, so much so that people started using the expression "Healthcare 4.0"[4] to refer to today's high degree of interconnection and sharing of data between patients, doctors, and healthcare facilities.[5] In this scenario, unauthorized sharing, and highly publicized breaches and robbery of sensitive data avidly erode the trust that people lay in healthcare institutions.[6] This is certainly a situation that commands rethinking and consideration of alternative approaches. Tools such as the groundbreaking blockchain technology, as well as systems based on artificial intelligence (AI), present great potential in this perspective.[7] According to Elisa Ficarra, AI is at a state of development such that it can offer technologies capable of modeling the complexity of medicine".[8] On the other hand, the use of new and disruptive technologies in the health domain can also result in pitfalls: complex and unusual ethical problems concerning the care and treatment of patients, risks related to the possibility that someone will hack the systems, as well as critical profiles in terms of protection of the data collected. Hence the need for interventions by the legislator with the aim of regulating these aspects in a way that is more adherent to day-to-day concrete experiences. In this regard, it seems worth to recall the issue of tangible and intangible infrastructures, which must allow, as the European Parliament has affirmed, equal access for all citizens to these innovations, tools, and technological interventions.[9]

1.1. *Genetic data*

In the present paper, the focus is on the protection of personal data in health research. In such a context, therefore, we are dealing with genetic data.

The study of genetic data is of great importance not only for the subject to which the data refer, but for the community as a whole. And indeed, now more than ever, a significant degree of interest can be found in sharing information for research purposes.

We can identify two opposing sides of genetic data. On the one hand, they constitute a very precious resource for the development of science among humans: it is indeed possible, by studying genetic information, to deepen the knowledge of pathologies and consequently predict the onset of diseases and ensure the possibility of intervening in advance on them; on the other hand, however, it is a particular category of personal data that plunges into the most intimate sphere of the people.

This polymorphic nature becomes even more evident if we take a quick look at some

ley-Fletcher, *Digital healthcare: new scenarios and new professions*, in *Astrid Rassegna*, vol. 18, 2016, 1.

[3] In this connection R. Ducato, *Database genetici, biobanche e "health information technology"*, G. Pascuzzi (ed.), in *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, 305-320.

[4] On this topic, P. Jayaraman, A.R.M. Forkan and A. Morshed, *Healthcare 4.0: A review of frontiers in digital health*, in *WIREs Data Mining and Knowledge Discovery*, vol. 10, 2019, 1-23; see also J.J. Hathaliya and S. Tanwar, *An exhaustive survey on security and privacy issues in Healthcare 4.0*, in *Computer Communications*, vol. 153, 2020, 311-335.

[5] E. Coiera, *Guide to Health Informatics*, Sydney, CRC Press, 2015. See also J. Hathaliya, P. Sharma and S. Tanwar, *Blockchain-based Remote Patient Monitoring in Healthcare 4.0*, presented at 2019 *IEEE International Conference on Advanced Computing, IEEE (Institute of Electrical and Electronics Engineers)*, 13-14 December 2019, especially 87.

[6] A. Hasselgren, K. Kralevska and D. Gligoroski, *Blockchain in healthcare and health sciences - A scoping review*, in *International Journal of Medical Informatics*, vol. 134, 2020, 4.

[7] It has been noted that the use of artificial intelligence "understood as the massive and targeted use of algorithms and of data analysis techniques to guide the behavior of human beings with the declared purpose of preventing disease, is playing an increasingly important role, connected but different from the search for new forms of therapy, new medicines, new treatment technologies". R. Bifulco, *Intelligenza Artificiale, internet e ordine spontaneo*, in F. Pizzetti (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Turin, Giappichelli, 2018, 383 ff., especially 386; see also A. Spina, *La medicina degli algoritmi: Intelligenza Artificiale, medicina digitale e regolazione dei dati personali*, in F. Pizzetti (ed), *Intelligenza Artificiale*, 319 ff.

[8] E. Ficarra, interview in the context of FocusUnimore newsletter article *Dati sanitari: anche una docente Unimore nel gruppo di lavoro dell'Healthcare Data Innovation Council, al servizio della Comunità Europea*, in FocusUnimore, July 2022, n.28, available at www.focus.unimore.it/luglio-2022.

[9] European Parliament, *Resolution of 16 February 2017 on improving the functioning of the European Union building on the potential of the Lisbon Treaty*, Strasbourg, Point 40, where the Parliament asks the Commission and the Member States to promote the development of assisted technologies in order to favor the development and adoption of these technologies by subjects who need it, in accordance with art. 4 of the UN Convention on the Rights of Persons with Disabilities, which the Union has signed.

legal sources: the principle of benefit-sharing, affirmed by the UNESCO Declaration on the Human Genome,[10] and the right to free scientific research, already affirmed by articles 9 and 33 of the Italian Constitution and most recently reaffirmed at the UN[11] would seem to imply a *favor* for a freer use of genetic data rather than for an enforcement of the stringent regulations on privacy protection, which impose significant precautions on health facilities and laboratories for the use of this peculiar type of data in research. The discipline relating to the protection of this category of data, in fact, "stands at the intersection between the protection of health, the freedom of research and scientific experimentation, and public safety, creating situations whose regulation requires complex operations balancing".[12]

Art. 9, par. 1 of the GDPR inserts genetic data (together with biometric data) among the "special categories of personal data" (the so-called "sensitive data") whose processing is prohibited, with the exceptions identified in the following paragraph. Genetic data (as well as biometric data) then became, on a legal level, a species of the sensitive data *genus*, so much so, as it is known, that it can be considered "super-sensitive" data.[13]

1.2. *Anonymization*

In the kind of research that involves the use of biobanks, the protection of the data subject (understood as the natural person who has provided human biological material) consists in protecting sensitive personal information by ensuring that, when processed, it is in fact impossible to identify the individual to whom those data refer. Such task is generally addressed by resorting to anonymization and pseudonymization procedures. However, it is now known that anonymization is often a partially reversible process. And indeed, anonymization usually consists in the loss of some attributes connoting the personal data, so that the latter no longer consists of information attributable to a subject. This elimination, however, is not always such as to totally exclude re-identification: data can undergo procedures that allow to re-identify the subjects to which they refer. Studies were made in this regard, and they have shown the possibility of re-identifying anonymized data sets.[14] These aspects have built a new vision of the relationship between personal data and anonymous data that is no longer binary, but rather a perspective that ranks these two types of data at the ends of a graduated scale where variability is given by how easy it is to re-identify the data.

1.3. *Data breach*

It should be emphasized that health databases possess peculiar traits: a large-scale health database is not just an up-scaled version of a normal data collection: indeed, biobanks generally bring together much larger and much more diverse sets of information and biological materials and, above all, the data present in a biobank bear a significantly higher value.[15]

[10] UNESCO, *Universal Declaration on the Human Genome and Human Rights*, adopted by UNESCO General Conference on November 11, 1997.

[11] The right to science and scientific progress as a human right has had a recent and decisive recognition at the UN, with the consequent burden on States to implement the tools for its implementation and protection. See United Nations Organization, Committee on Economic, Social and Cultural Rights, *General comment* n. 25 of 30, New York, April 2020, 6-7.

[12] A. Iannuzzi and F. Filosa, *Il trattamento dei dati genetici e biometrici*, in S. Scagliarini (ed.), *Il "nuovo" codice in materia di protezione dei dati personali*, Modena, Giappichelli, 2019, 116.

[13] These normative clarifications are very important because, prior to the entry into force of the GDPR, genetic data was an ill-placed concept. The notion of genetic data was formally extraneous to that of sensitive data, for they did not figure in their legal definition. And indeed, Directive 95/46/EC, relating to the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data (also known as the "mother directive"), did not recognize the specificity of genetic and biometric data and it therefore made them fall into the general category of personal data, that included "any information relating to an identified or identifiable natural person ("data subject")".

[14] According to the findings of the first Permanent Ethics Committee of the United States, as early as the late 1990s, the samples which were identified at the time of collection, even if subsequently coded or anonymized, inevitably maintained a certain level of re-identifiability. In this regard, see also S.N. Eshun and P. Palmieri, *Two de-anonymization attacks on real-world location data based on a hidden Markov model*, presented at *2022 IEEE European Symposium on Security and Privacy Workshops*, Genoa, 6-10 June 2022, 1-9.

[15] The value of Big Data, understood according to Doug Laney's paradigm of the "five v's" (volume, variety, velocity, value and veracity) could be the most important "v". There are those who point out that "the data [themselves are] the main object of entrepreneurial activity. The data (both personal and anonymous) [are] captured, conveyed, processed and for the most part stored and accumulated, representing a different and alternative form of 'capital' to the surplus value obtained from the sale of services or advertising space". G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità*

And indeed, it is precisely the considerable value of health-related data that has attracted the attention of numerous computer hackers who have been targeting patient data collections stored (in a more or less secure manner) in the archives of health facilities, thus configuring examples of the phenomenon known as data breach.[16]

It seems that, contrary to what one might expect, the attackers are not only eager to get hold of credit cards. In fact, more and more violations appear rather as preparatory acts for a different and more complex "criminal design": that of identity theft. Using spear phishing strategies, often by means of ransomware,[17] hackers ask for large sums of money in exchange for the medical records they hold hostage. Medical records are in fact a much more valuable "asset" than credit card data.[18] Indeed, if the latter end up in the wrong hands, they can easily and quicky be deprived of their effectiveness at the request of the owner; but the offense that moves through the medical records and health information of patients is more complex and insidious.

Such a scenario raises a lot of concerns, so much so that one wonders if it is possible to find new systems to collect and store data that would prove a more resistant solution not only to cyber-attacks (be them malicious or accidental) but also to the concrete risk of reversibility of the traditional anonymization procedures. Blockchain technology seems to have considerable potential precisely in these aspects.[19]

2. *The advent of Distributed Ledger Technologies (DLTs): characteristics of Blockchain*

Let's clarify the features of blockchain that are relevant to this analysis, in order to understand why this class of technologies promises a revolutionary innovation in the healthcare domain.[20]

First, it should be stressed that Blockchain is a particularly complex technology, aimed at carrying out various operations including transactions management and value exchange. It can be synthetically represented as a database that is distributed[21] among the users

della rete nel mercato transnazionale dei dati personali, in *Diritto dell'informazione e dell'informatica*, 2015, 911. See also D. Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, Stamford, CT, in *Gartner*, file 949, February 2001.

[16] Are data breaches frequent? 2019's Annual Report of the Italian data protection authority outlines noteworthy information in this regard: the panel chaired by Antonello Soro informs us that in 2019, in Italy, the Authority received as many as 1443 reports of IT incidents concerning personal data: this translates to nearly four data breaches per day. Only one year earlier, in 2018, 650 attacks had been registered (interestingly, of these 650 reports, 630 had occurred after 25 May, i.e., the date of entry into force of the GDPR which made reporting data breaches mandatory). See Garante per la protezione dei dati personali, *Annual report 2019*, Rome, 23 June 2020.

[17] The term "ransomware" refers to a class of malware (computer viruses) that makes the data on the infected computers inaccessible and asks for the payment of a sum of money (usually via *bitcoin*, *ethereum* or other cryptocurrency payment method, with the aim of rendering the transaction untraceable) to have them back.

[18] Ponemon Institute's 2016 Annual Report efficiently illustrates the data-breach scenario in the medical sector, outlining that data breaches in healthcare are increasingly costly and frequent, and continue to put patient data at risk. Based on the results of this study, it is estimated that data breaches cost the healthcare industry $6.2 billion, and during the two-year span before the report the average cost of a data breach for healthcare organizations was estimated to be more than $2.2 million. "No healthcare organization, regardless of size, is immune from data breach". Ponemon Institute, *Benchmark Study on Privacy & Security of Healthcare Data* (Annual Report 2016), 1.

[19] On the usefulness of blockchains from a health-data breach perspective, see Vv.Aa., *Blockchain: Opportunities for Health Care*, Deloitte, August 2016, 6: "An interoperable blockchain can strengthen data integrity while better protecting patients' digital identities […] Each participant connected to the blockchain network has a secret private key and a public key that acts as an openly visible identifier. The pair is cryptographically linked such that identification is possible in only one direction using the private key. As such, one must have the private key in order to unlock a participant's identity to uncover what information on the blockchain is relevant to their profile. Therefore, the blockchain public/private key encryption scheme creates identity permission layers to allow patients to share distinct identity attributes with specific health care organizations within the health care ecosystem on as-needed-basis, reducing vulnerabilities […] on all sides and allowing for data access time limits to be introduced by patients or providers"; on the usefulness of blockchain for anonymization, see F.J. De Haro-Olmo, A.J. Varela-Vaca and J.A. Álvarez-Bermejo, *Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review*, in *Sensors*, vol. 20, issue 24, 2020, 7171.

[20] In this connection, Vv.Aa., *Blockchain: Opportunities for Health Care, Deloitte*, August 2016, especially 5.

[21] The distribution of a database among the users of an installment represents the distinctive feature of the so-called distributed ledger technologies (DLTs), of which the blockchain is the most famous example. The concept of distributed ledger is opposed to the traditional logic of centralized data management (for example, financial institutions, public bodies, health research structures, etc.), subject to the control of one single and superordinate central authority. In DLTs there is no hierarchical order: all network users are at the same level and can only act with the consent of the majority.

of a network.[22] More specifically, blockchain consists of a public and shared ledger capable of automatically update on each node[23] participating in the network. This ledger is structured in blocks, each of which represents a number of transactions whose origin and time of execution are indelibly and immutably set through an asymmetric key-encryption mechanism and a timestamp. Each block is irreversibly linked to the previous one through a particular logarithmic operation, the so-called hash function,[24] and forms the chain of blocks.

It must be emphasized that, in principle, there is no such thing as "the" blockchain. It is in fact a class of technologies that have different technical properties and different rules. In this analysis, when the expressions "blockchain(s)" and "blockchain technology" are used, they refer to a class of technologies that can take many possible different forms, but generally share a few general principles. Therefore, when trying to determine if a specific blockchain, used in a specific context, is compliant with the GDPR, it is nonetheless necessary to investigate the precise characteristics of that blockchain, used in the specific case.

2.1. *The health sector*

In recent years, blockchain technology has become very trendy and has penetrated different domains, mostly due to the popularity of cryptocurrencies. A sector in which blockchain technology has a significant potential in terms of data protection is that of healthcare, to the extent that the data used in this field (genetic data), as we have seen, possess characteristics that distinguishes them from any other type of data. Furthermore, healthcare is a field where the ability to connect many different systems quickly and safely is of central importance, not to mention the need for great accuracy in the preparation and management of electronic healthcare records (EHR). In the health domain, to both maintain the patients' privacy and exchange data with other institutions in the healthcare ecosystem, access control, provenance, data integrity and interoperability are indeed crucial.

2.2. *Decentralization, disintermediation, immutability*

There are two main reasons why blockchain is being touted as a groundbreaking conception that will fundamentally change many sectors and perhaps the entire economy. First, blockchain is based on the principles of decentralization and disintermediation. This means that blockchain allows for the exchange of data in an environment that is devoid of a superordinate "governor"; and in a direct manner, i.e., without the need for an intermediary. Decentralization and disintermediation have made blockchain the technology of choice for creating cryptocurrencies. Cryptocurrencies allow for the direct transfer of value from person to person by bypassing traditional intermediaries such as banks and, in doing so, disrupt the traditional financial system and the financial industry.

Second, the technology behind blockchain provides near-absolute reliability, anonymity, and immutability of the data records. Participants in blockchain transactions do not have to know or trust each other to take part in a transaction. Instead, participants rely on encryption and block-immutability to protect their data and to secure themselves from counterparty pitfalls. The data inside the blocks are accessible only to those in possession of cryptographic keys and, in the case of blockchain without authorization (*private and permissioned*, as will be seen shortly), the immutability of the data is guaranteed by the fact that it is necessary to obtain consent from all the participants not only to add new blocks to the chain, but also to remove them (and we will also see that

[22] See L. Parola, P. Merati and G. Gavotti, *Blockchain e smart contract: questioni giuridiche aperte*, in *I Contratti*, issue 6, 2018, 681 and seq.

[23] In information technology and telecommunications, a node is any hardware device capable of communicating with the other devices that are part of the system; it can be a computer, a printer, a fax machine, a modem, etc. In blockchain's specific context, a node is a computer connected to the blockchain network that stores a copy of the public ledger.

[24] The hash function transforms data of arbitrary length (i.e., a message) into a fixed-sized binary string called a hash. In blockchains, each block is identified with a hash which, through an alphanumeric string of a given length, summarizes and encodes the information relating to the transactions it contains. When adding a new block to the chain (containing new transactions originating from those contained in the previous block), the hash function will have as its object the information relating to the new transactions together with the identifying hash of the previous block. Basically, each new hash will also enclose the hash of the previous block, thus creating an indissoluble chain.

erasure and even "mere" modification of blockchain data represents a particularly laborious operation). Data ledgers in the blockchain can be suitable to store any type of information, so the technology can be used for nearly any kind of data-processing purpose.[25]

2.3. *The "resilience by replication" principle and the append-only nature of blockchain*

So, in essence, blockchain is a shared and synchronized digital database: therefore, it is essentially a database that does not exist in one place only, rather, it exists in parallel on many different computers and all these computers share the complete copy of the entire dataset present on the database. Those computers can be in many different places and, consequently, many different jurisdictions, which brings with it many legal issues. Blockchain precisely intends to pursue the resilience of the information contained in it through its replication, i.e., by replicating and storing data on many different servers. The idea is that even if some of those computers stop working, suffer malfunctions, or are destroyed, it is still possible to keep the database as such, as it exists in many different places.[26]

Another very important feature of the blockchain, especially from a GDPR perspective, is that it is an append-only database: a database in which one can only store data, because destruction or alteration of the data happens only in extraordinary circumstances and moreover, is very difficult to achieve. Another interesting feature of this class of technologies is the use of timestamps that contain a mechanism to track who carried out an operation and at what exact time.

2.4. *Public and private blockchains*

Blockchains are essentially divided into three categories. First of all, there are *public and permissionless* blockchains and there are *private and permissioned* blockchains. Basically, the difference is that public blockchains contain data (in most cases, encrypted or hashed) that are visible to all who want to access it; in the private blockchain, however, this is not the case. The difference lies in the fact that, in order to enter the network and add data to it, in the public type of blockchain it is not necessary to obtain the permission of anyone to do so, whilst in the permissioned-systems there is generally a central and superintendent subject (the so-called gatekeeper), who decides which parties can join the blockchain ledgers. Then, a third type of blockchain exists, and it is a *tertium genus* that sits halfway between the first two aforementioned types: it is in fact called *public-permissioned*, also known as *consortium*. Consortium-type blockchains allow only a selected group of nodes to participate in the distributed consensus process.[27] When a consortium-blockchain is established within a sector (for example, the healthcare, financial or insurance sector), it is opened for limited public use, which is partially centralized. Moreover, even for a consortium between organizations (for example, healthcare facilities, financial companies, government institutions) open for public use, it is still necessary to maintain trust mechanisms with a certain degree of centralization. It has been reported that the consortium-type blockchain appears to be the preferred design choice for health facilities.[28] And indeed, since healthcare-information systems deal with highly sensitive data, (which usually imply that a small number of entities should have access to them) a consortium blockchain may be more appropriate than an unauthorized public one to ensure that data are not accessible by those who have no rights to view them, while maintaining an appropriate degree of publicity motivated by public interest in research and

[25] For example, blockchains can be used as a good tool for identity management purposes. See K. Shraddha, *Building-Blocks of a Data Protection Revolution - The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, in *MIPLC Studies* (Munich Intellectual Property Law Center), vol. 35, 2018, 31-33.

[26] On this topic, see N. Al Azmi, G. Sweis and R. Sweis, *Exploring Implementation of Blockchain for the Supply Chain Resilience and Sustainability of the Construction Industry in Saudi Arabia*, in *Sustainability*, vol. 14, 2022; G. Li and J. Xue, N. Li, *Blockchain-supported business model design, supply chain resilience, and firm performance*, in *Transportation Research Part E: Logistics and Transportation Review*, vol. 163, July 2022.

[27] Z. Zheng, S. Xie and H. Dai, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, presented at 2017 IEEE International Big Data Congress, IEEE, Boston, MA, 11-14 December 2017, 557-564; M. Hölbl, M. Kompara and A. Kamišalić, *A Systematic Review of the Use of Blockchain in Healthcare,* in *Simmetry*, vol. 10, 2018, 470.

[28] A. Hasselgren, K. Kralevska and D. Gligoroski, *Blockchain in healthcare and health sciences - A scoping review*, 7; on this topic, see also E. Coiera, *Guide to Health Informatics*, Sydney, CRC Press, 2015.

the progress of medical science.

3. *Antinomies between Blockchain and GDPR: centralization vs decentralization; mutability vs immutability; data minimization*

Is there a way to reconcile the potential of blockchain technology with privacy regulation? How could blockchains be used in a way that is compliant with the GDPR?

An effective way to approach these questions is the following: instead of focusing immediately on how to force blockchains within the scope of the GDPR, one could analyze the GDPR using the blockchain as a key to understanding and, therefore, learning many interesting things on the GDPR itself. The first element that emerges from a reading of this type is a strong tension between the two players at stake: the GDPR and blockchains.

There are two general reasons why this tension, that has caused much controversy amongst media, scholars and even regulators, exists. First, as mentioned, blockchains generally decentralize data on different computers and this in turn decentralizes the governance of the blockchain. There are some implicit assumptions in the legal framework of the GDPR: one of these is that there will generally be one legal entity responsible for a specific set of data; this is, generally, not the case when using blockchains.

The second general tension that lies between this technology and the GDPR corresponds to the contrast between the mutability required by the GDPR and immutability, a fundamental characteristic of the blockchain. And indeed, the GDPR contains the obligation to change or delete data when the data subject requests for it. The problem is now the following: usually, blockchains are specially-designed to make said operation impossible or at least very difficult. That tension is manifested across different points of the GDPR.

One of the fundamental principles of the GDPR is the so-called *data minimization principle*: art. 5, par. 1 letter c) states that personal data are adequate, relevant, and limited to what is necessary with respect to the purposes for which they are processed. The idea is that you need to minimize the data you are using in a specific context. And there are two reasons this is difficult to achieve in a blockchain environment. The first reason is that the databases of a blockchain are continuously growing and, essentially, no data can be deleted;[29] the second reason concerns the aforementioned paradigm of resilience by replication: not only do data keep growing, but said data are also being replicated on many different computers, thus giving rise to copies of data everywhere.

Similar tensions can be identified when observing the purpose limitation principle pursuant to art. 5, par 1, letter b) of the Regulation: this tells us that personal data must be collected for certain explicit and limited purposes and cannot be further processed in a way that is incompatible with those purposes. Now, the addition of data to blockchain often serves a specific purpose, such as a transaction. But this is just the initial purpose. What happens next is that the data continues to be stored in the blockchain, and it is known that even data retention alone qualifies as data processing from a GDPR perspective.[30] Therefore, the question arising is whether from a GDPR-perspective it could be argued that not only the initial purpose of the transaction, but also the secondary use (represented by the "maintenance" of data) constitutes data processing. The answer to this question is not entirely clear as the notion of purpose limitation has not yet been interpreted in a way that is adequately corresponding to the blockchain dynamics.

3.1. *Right to erasure*

Then, there is the tension that has gotten the most attention so far. It is the obligation pursuant to art. 17 GDPR, which requires the deletion of data in certain circumstances;[31] it

[29] For this characteristic, as already mentioned, blockchains are usually described as an "append-only database": a database where, essentially, you can only add data, which will remain permanently stored.

[30] Not to even mention that further processing would also take place each time the network reaches the conditions for new data to be added.

[31] The circumstances in which the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay are the following:

(1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(2) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(3) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate

is the right to erasure, also known as the *right to be forgotten*. Art. 17 GDPR states that the data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay. Now, to determine whether the obligation of Article 17 can actually be met in a blockchain environment depends significantly on how the term "erasure" is to be interpreted from a GDPR perspective.[32] Therefore, on the one hand, it could be argued that erasure (which is neither defined in the Recitals nor in the legislative text of the GDPR) is to be interpreted with its literal meaning. However, this does not appear if you look at the Google Spain ruling of 2014:[33] in this judgment, the issue was not about deleting data, but about disconnecting search results from Google's search algorithm. Therefore, this judgment could be interpreted as meaning that there are situations in which a true erasure (in the sense of a total cancellation) of data is not necessary in order to fulfill the obligation of art. 17, as this was not in dispute within this judgment. And indeed, the Court of Justice ruled that European citizens have a right to request that commercial search engines, such as Google, should remove links to private information when asked, provided the information is no longer relevant.

Moreover, when looking at what the various data-protection Authorities have stated on this issue, it appears that there is no agreement between them on how to interpret the term "erasure". The British ICO, for example, has been arguing for several years now that putting data "beyond use"[34] is equivalent to deleting data for the purposes of Article 17 of the GDPR. In this regard, the French data protection Authority suggested that, to comply with the obligation pursuant to art. 17 in the blockchain context, it is not necessary to erase the data but, rather, alternative means could also do. The concrete example that the French guarantor suggests is the following: since blockchains are made up of encrypted data that can only be reached through a key, the private key needed to access the ledgers could be destroyed, thus performing out an operation that is in fact equivalent to the erasure of the data.[35] This is the mechanism that is used today by several biobanks, as will be seen later in the discussion, precisely to be compliant with the *right to be forgotten*.

4. *The twofold difficulty when dealing with data controllership in Blockchain environments: identification and obligations*

Another very interesting yet controversial area of privacy law to look at through the lens of blockchain technology is that of the data controller, and in particular its identification. Blockchains are polycentric networks where we have many actors influencing the processing of data. Art. 4 par. 7 GDPR informs us that the data controller is the natural or legal person, public authority, agency, or other body which, alone or together with others, determines the purposes and means of the processing of personal data. GDPR also contains the notion of joint controller: art. 26, par. 1 of the Regulation

grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(4) the personal data have been unlawfully processed;
(5) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(6) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

General Data Protection Regulation (GDPR), Article 17: *Right to erasure ("right to be forgotten")*.

[32] On the right to be forgotten, see S. Scagliarini, *Digital identity and privacy protection*, presented at Pisa Group Association's Annual Conference, Genoa, 18-19 June 2021 "Constitutional law and the challenges of technological innovation" , 9 *et seq.*: article 17 of the GDPR has been criticized as it reduces the discipline of the right to be forgotten to the mere "cancellation" of data; but, as clarified by the Italian Supreme Court in the decision no. 19681/19, "when dealing with the right to be forgotten we are actually referring to at least three different situations: that of those who wish not to see a second publication of news (that were legitimately spread in the past) relating to events, when a certain time has passed between the first and second publication; that, connected to the use of the internet and the availability of news online, consisting in the need to place the publication, which legitimately took place many years earlier, in the current context [...]; and that, finally, dealt with in the Google Spain ruling of the European Court of Justice, in which the data subject asserts the right to have data deleted".

[33] European Court of Judgment, Judgment of the Court (Grand Chamber) of 13 May 2014. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

[34] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR), Right to erasure*.

[35] National Commission on Informatics and Liberty (Commission Nationale de l'Informatique et des Libertés - CNIL), *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*, November 6, 2018.

states that it is possible to have two or more controllers in a data-processing situation. This occurs when two or more controllers jointly determine the purposes and means of the processing.

This is indeed a very hot area of privacy law right now, to the extent that there have been several recent judgments where the European Court of Justice has interpreted the notion of joint controllership in interesting ways. For example, in the *Wirtschaftsakademie schleswig holstein* case,[36] the court essentially indicated that when a person accepts the means and purposes of data processing that have been specified by someone else, and then benefits from this agreement in some way, it can be assumed that that person also actively determines the means and purposes of data processing and consequently becomes a data controller. This orientation was confirmed, only a few weeks later, in a case relating to Jehovah's Witnesses[37] in which the Court reaffirmed this reasoning based on this interpretation of the notion of joint controllership: the Court also added that, to be a data controller, it is not necessary to have physical access to the personal data in question. Again, the court indicated that a natural or legal person who exercises an influence on the processing or on personal data for their own purposes can be considered a data controller. So, recent case law on joint controllership embraces a very broad view of the concept; it can then be affirmed that anyone who consents to someone else's data processing and then takes advantage of it for their own purposes becomes the data controller.

The question arising is what this broad definition of both controllership and joint controllership could mean in the blockchain context. In this regard, the French Authority (CNIL) released a document in 2018 in which they stated that participants, who have the right to "write" on the chain and who decide to send data for validation by the miners (which will be discussed shortly), can be considered as data controllers.[38]

4.1. *Actors of blockchain*

There are several actors that participate in blockchain networks and that could, as a matter of principle, be in possession of the requirements to be qualified as data controllers. Can, for instance, core developers be considered as data controllers? Core developers are the people who create the software, the real IT structure on which a particular blockchain network is based. It may seem that core developers cannot be really considered data controllers since, while retaining a decisive influence on the means insofar as they determine the appearance of the software (therefore they certainly have a say), the objective of their role is usually that of assigning powers and responsibilities to other stakeholders such as, for example, directors, through IT programming. Furthermore, the actual personal data does not pass through the IT systems of the core developers. In short, they limit themselves to supplying the technology.[39] However, this does not necessarily exclude that they may be joint controllers. In the case of *Jehovah's Witnesses*, for example, the European Court of Justice has decided that it is not necessary for all joint controllers to have access to personal

[36] European Court of Justice, Judgment of the Court (Grand Chamber) of June 5, 2018: *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* in relation to whether an administrator of a fan page on a social network qualifies as a joint controller with regards to the processing of personal data of visitors to the page and the competence of a supervisory authority. The CJEU held that an administrator of a fan page hosted on a social network must be regarded as a controller under Article 2(d) of the Data Protection Directive 95/46/EC.

[37] European Court of Justice, Judgment of the Court (Grand Chamber) of 10 July 2018, *Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta,* where the Court has held that religious groups undertaking door-to-door preaching activities in specific geographical areas were subject to the Data Protection Directive (95/46/EC).

[38] According to the French Authority, indeed, blockchain participants define the purposes (objectives pursued by the processing) and the means (data format, use of blockchain technology, etc.) of the processing. More specifically, the CNIL considers that "the participant is a data controller: when the said participant is a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e., when the activity is not strictly personal); when the said participant is a legal person and that it registers personal data in a blockchain". National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés - CNIL), *Solutions for a responsible use of the blockchain in the context of personal data*, September 2018, available at www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

[39] M. Schellekens, *Conceptualizations of the controller in permissionless blockchains*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 11, 2020, especially par. 47.

data.[40]

Then we have the so-called *miners*. The miners are those who accumulate cryptocurrency on their computers, the so-called *farms*, which are computers entirely dedicated and adapted for this purpose. They have, in the same way as developers, a decisive influence on the means also because of their active role in the governance of the blockchain but, still in almost all cases they do not have an influence on the purposes of data processing.[41]

Then there are the *nodes*, which are the many computers in which the blockchain is stored. There is relatively broad agreement that nodes could qualify as data controllers[42] insofar the nodes determine their purpose for participating in the network and to the extent that they have access to all data stored in the ledgers. However, the possibility of defining nodes as controllers is disputed.[43]

What emerges is that to identify the data controller in a blockchain environment is a laborious task. To fulfill this task, it is necessary to investigate the precise characteristics of the blockchain used in the specific case of use; the data controller (or controllers) must be identified on a case-by-case basis.

[40] European Court of Justice, Judgment of the Court (Grand Chamber) of 10 July 2018, *Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta.*

[41] This view is confirmed by the French data Authority (CNIL) in its 2018 document precisely in the sense that "miners are only validating transactions submitted by participants and are not involved in the object of these transactions: therefore, they do not define the purposes and the means of the processing", National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés - CNIL), *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*, 6 November 2018; See also M. Schellekens, *Conceptualizations of the controller in permissionless blockchains*, par. 17.

[42] On this topic, M. Florian, S. Henningsen and S. Beaucamp, *Erasing Data from Blockchain Nodes*, presented at 2019 IEEE European Symposium on Security and Privacy Workshops, IEEE (Institute for Electrical and Electronics Engineers), 17-19 June 2019, 367-376; see also J. Czarnecki, *Who is the data controller in a blockchain?*, in *Newtech Law Blog*, August 20, 2018; and C. Andronicou, *Blockchain and the GDPR: Clash of the Titans*, in *International Network of Privacy Law Professionals*, August 2021.

[43] In this connection, P.J. Pesch and C. Sillaber, *Distributed ledger, joint control? - Blockchains and the GDPR's transparency requirements*, in *Computer Law Review International*, vol. 17, 2017, 166 ff.; See also M. Berberich and M. Steiner, *Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers*, in *Eur. Data Prot. L. Rev.*, 2016, vol. 2, 422 and seq.

4.2. *Obligations*

After investigating who can be considered the data controller, the second question is: what does it mean, for a subject, to actually be the data controller in a blockchain environment? The first thing to point out is that, none of the actors we have examined have full control of what happens to the personal data present on the blockchain network. So, for example, if one were to accept that the node is the data controller in relation to the personal data stored on the blockchain, the node will not be able to realize the right of access pursuant to art. 15 GDPR, since all nodes will be encrypted with the hash function and this could constitute a major obstacle to comply with GDPR's obligation of correctly supplying information to the data subject about his or her data; in the same way, then, the nodes will never be able to operate independently pursuant to the right to be forgotten *per* art. 17.

A very interesting element that highlights the factual inability of these actors to comply with the obligations imposed by the GDPR, and which motivates the tension between the GDPR and blockchain, can be found under art. 26 GDPR: its first paragraph states that, where there are joint controllers who determine in concert the purposes and means of the processing, they must conclude an agreement that establishes their respective responsibilities. Therefore, the third paragraph of article 26 adds that "regardless of the provisions of the agreement referred to in paragraph 1, the data subject may exercise his rights pursuant to this regulation towards and against each data controller".

So, if we consider that in blockchains (in particular the public and permissionless types) there are many different actors and several of these can actually qualify as data controllers, a question spontaneously arises: who of those many parties should actually address the data subject and what happens if the latter decides to contact one of the joint data controllers who is in fact unable to fulfill the obligation imposed on him under the GDPR? Even this, in the absence of an *ad hoc* discipline, will be assessed on a case-by-case basis. It is certain that in private and permissioned blockchains (but also in consortium-type blockchains) the solution could be less strenuous, since networks of this type are characterized by well-defined governance structures, capable to establish the roles of the different actors and

the interactions between them; more difficult, on the other hand, is to navigate within the framework of public and permissionless blockchains.

5. *"Block" biobanking perspectives and advantages for healthcare*

We have analyzed the relationship between the GDPR and blockchains focusing exclusively on its tensions and contrasting elements. Before concluding, however, it is also appropriate to focus on the positive aspects of the relationship between Europe's main law source on privacy and the revolutionary blocking technology. Of course, the current debate focuses more massively on the discord that exists between them, but people are also starting to realize that blockchain is really a tool that could bring a variety of benefits and that it is totally capable of contributing to the development and enrichment of the very culture of privacy regulation. Let's see how this is possible by using the healthcare domain as a key to understanding.

Blockchain is a class of technologies that can be exploited in several ways. However, we have noticed how it is not to be understood as a technology that is automatically useful for the protection of personal data nor automatically advantageous for the goals of the GDPR. However, it is a very malleable technology and, when molded in the right shape, it can help accomplish some of these goals (e.g., to adapt to the GDPR, it appears crucial to opt for a private and permissioned blockchain model or, at least, a public-permissioned consortium).

Some uses of blockchain can be beneficial with regard to the aspects of accountability and transparency. Having a ledger that is distributed among many different actors, equipped with a timestamp and whose operation is based on extremely rigid parameters of automaticity and certainty, could be the ideal tool to keep track of the obligations that the data controllers must put in place to comply with the GDPR in the phases of the data processing impact assessment (DPIA), so that they can demonstrate that they have acted in accordance with their obligations, complete with certain date; it could function as a guarantee system through which data subjects can monitor who has had access to their data and at what time, and with which they can quickly and accurately obtain all the information they are entitled to pursuant to art. 15 GDPR, with grand benefits from a transparency point of view; or again, it could be greatly helpful for the collection of consent to the processing of data.

5.1. *Examples of blockchain-based biobanks in practice*

In this regard, there are several examples of biobanks that have been conceived precisely in this spirit, namely the search for a use (and, even before, a modeling) of blockchain as adherent as possible to both the dictates of the GDPR and the special needs of medical research. A research group from the University of Malta has devised, in the context of biobanks, a solution based precisely on the aspects of gathering consent and that even aims to solve the apparently diabolical problem of blockchain's compliance with the right to be forgotten, and published their solution in Nature.[44] The researchers talked about dynamic consent. Dynamic consent aims to give people the opportunity to be better informed about their consent choices and, in general, about the ongoing research process, and to maintain guarantees and control over how their biological samples and data are used. This consent system would also allow research participants to access a record of their consent decisions. Participants can review previous decisions and change their decision. In other words, even if the participant signed a consent form at the beginning of the process, that would not be the last word on his or her consent status. They can, in fact, update or withdraw their consent at any time. Therefore, this peculiar biobank, called Dwarna, allows research partners to learn more and get involved in genomic research. Search Partners log into the Dwarna Portal using their alias and password to learn about ongoing searches. If they are inclined to participate in any study, they can indicate it by flipping a switch for consent. They can also withdraw this consent at any time using an identical mechanism or request the deletion of their data and the destruction of their bio-sample from the biobank. But the examples of blockchain-based biobanks are

[44] For Dwarna's white paper, see N. Mamo, G.M. Martin and M. Desira, *Dwarna: a blockchain solution for dynamic consent in biobanking*, in *European Journal of Human Genetics*, vol. 28, 2020, 609-626.

several:[45] MedRec[46] is also (mainly) a blockchain solution that stores sensitive personal information in a more traditional and centralized off-chain database from which data can be removed. The blockchain itself only stores the hashes of this data and preserves a ledger containing patient permissions to doctors to access the data.

5.2. *Other beneficial uses of blockchain for patient care*

And indeed, blockchain technology can be of great help for access control, management of medical records and their sharing, but also for verifying the correctness of the financial statements and procedures of a healthcare company. Undoubted benefits have also been found in the pharmaceutical field, where it is necessary to manage drug prescriptions with great precision and it is essential to better organize drug supply chains, according to parameters of certainty and efficiency.[47] Furthermore, in the field of healthcare, the aspect of the patient's control over his health data and the relationship between patient and doctor is of central importance, and indeed, blockchain opens new horizons also with regard to Remote Patient Monitoring (RPM), namely the set of advanced systems that allow doctors to obtain real-time information on their patients remotely with the help of the wireless-communication system, with the effect of reducing time and costs for the patient, and also providing medical assistance of quality to the patient.[48]

In the digital age, preserving patient data privacy is crucial. The data present in the collections of healthcare facilities, as we have seen, are very sensitive and very expensive. Therefore, they represent a primary target for cyber-attacks. Blockchain technology is indeed very robust against attacks and failures and provides several access control methods.

5.3. *Blockchain in health data protection: conclusions*

Blockchain seems to have all the credentials to protect data and improve the quality of patient care. Its cornerstones, based on shared immutable data organized in a network of nodes where transactions are stored in a digital ledger, have already been applied in many sectors such as banking and finance to protect data from intruders. There are various applications in the health field, such as for Electronic Health Record (EHR), for genomics, biomedical, pharmaceutical science, and laboratories in which the blockchain is integrated with existing applications or provides the tools to create new ones. Therefore, it seems that blockchain, used in a virtuous and targeted way, paints a picture full of positivity regarding health data and healthcare as a whole.

Examples like these really highlight how the arguments supporting the total discord between blockchains and the GDPR and the absolute uselessness or even dangerousness of this class of technologies with respect to privacy regulation really lack vision and indeed constitute an obstacle to one of the very guiding principles of the GDPR itself, which is to support the development of technology, through principles and tools that can adapt to the rapid and, often, even subversive changes of society typical of this era of the digital economy. However, the study highlighted that blockchain is a multiform, malleable, and changing class of technologies, with technical characteristics and governance arrangements that can be very different from each other. For this reason, the compatibility of these tools with the Regulation can only be assessed on a case-by-case basis: just as it can be modeled in a beneficial and risk-free form, blockchain can also take on shapes that put a strain on the principles of privacy regulation, which are highly worthy of being taken into consideration as a reflection of common sense, as well as of commendable interest and effort by European legislators towards the

[45] In fact, just three years after what is conventionally identified as the birth date of the blockchain (Satoshi Nakamoto's 2008 white paper), Estonia had already partnered with the private sector to begin archiving medical records in blockchains. Since then, more use cases of blockchains in the healthcare sector have emerged in the literature. See M. Mettler, *Blockchain Technology in Healthcare: The Revolution Starts Here*, presented at 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, September 2019, 2.

[46] For MedRec's white paper, see A. Ekblaw, A. Azaria, J.D. Halamka and A. Lippman, *A case study for block-chain in healthcare:"MedRec" prototype for electronic health records and medical research data*, presented at *IEEE Open & Big Data Conference*, 22-24 August 2016.

[47] On this topic, A.D. Shetty, S. Shenoy and D. Sreedhar, *Traceability of counterfeit drugs in pharma supply chain through Blockchain Technology - A Systematic Review of the Evidence*, in *Research Journal of Pharmacy and Technology*, vol. 15, February 2022.

[48] J. Hathaliya, P. Sharma and S. Tanwar, *Blockchain-based Remote Patient Monitoring in Healthcare 4.0*, 87.

noble dreamscape of data protection.

6. *Concluding thoughts: should blockchain be considered an enemy or an ally of the GDPR?*

What emerges when analyzing blockchains from a GDPR perspective is an undoubted climate of tension. This tension can essentially be linked to two main antinomies: the antinomy between the centralization, on which the regulatory pattern of the GDPR is built (identification of a data controller, i.e., a center of imputation of obligations to be performed towards the data subject, according to the privacy-by-design and by-default[49] principles) and decentralization, major bulwark of the blockchains, which generates considerable problems regarding the configuration of responsibility under current privacy law; the antinomy between the mutability, required for the purposes of GDPR's *right to be forgotten*, and the immutability of blockchain ledgers, contained in realistically-indecipherable algorithms. These arguments have not escaped the attention of regulators and a whole range of experts in this sector. These factors have triggered a debate about whether the GDPR stands in the way of an innovative EU-based blockchain ecosystem. Some have expressed their support for a revision of the GDPR, and claim that blockchains should benefit from an altogether exemption of the EU data-protection framework. According to those, in fact, the very existence of the GDPR would stifle the free development and potential of blockchain in Europe, and this could leave Europe behind other jurisdictions on the planet which, not having the "burden" of the GDPR, will be able to exploit all the advantages of the novelties that this technology has in store for humans.[50] Others stressed the primacy of regulation and said that if blockchain can't comply with the GDPR, that means it is likely to be an innovation that should be abandoned as it is unable to achieve established public-policy goals.[51]

So, do we really need to change or even abolish the GDPR in an attempt to make Europe a competitive environment for data-driven economies, or should we leave blockchain technology stranded, given its apparent inability to comply with the law? Neither of these is the case or, rather, the solution lies somewhere in the middle. The GDPR is a principle-based regulation and has a whole range of regulatory mechanisms that were designed precisely to encourage the emergence of new technologies, such as certification mechanisms.[52] Furthermore, many of the existing tensions are basically reduced to simple lack of sufficient specification in the text of the law, or interpretation gaps. If we had more indications from the regulatory authorities, for example, on how the term "erasure" is to be interpreted in accordance with the specificities of DLT structures, together with a contribution from the people who develop and prepare blockchain networks aimed at setting up more "friendly" governance mechanisms (in the sense of taking into account the inevitable arrival of a regulatory eye that will, quite understandably, be looking for guarantees on the processing of personal data) it may well be possible to overcome those tensions that today represent a wall.

On the other hand, however, while there are certainly many tensions between different key features of blockchains and some cornerstones of European data-protection legislation, many of the related uncertainties should not be traced back only to the specific characteristics of this technology. Rather, by moving the magnifying glass to the GDPR, it can be highlighted that parts of it are to be

[49] The principles of privacy-by-design and privacy-by-default are dealt with in art. 25, paragraphs 1 and 2, GDPR. Recitals 24-29 define the techniques and measures to be implemented to ensure their compliance. In this regard, M. Midiri and S. Piva, *L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali*, in *Il "nuovo" codice in materia di protezione dei dati personali*, S. Scagliarini (ed.), 33.

[50] European Parliament - Panel for the Future of Science and Technology in the context of European Parliamentary Research Service (EPRS), *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, July 2019, especially 1.

[51] D. Meyer, *Blockchain technology is on a collision course with EU privacy law*, in *The Privacy Advisor*, 27 February 2018, blog article available at https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.

[52] Through the certification mechanism, data controllers obtain and benefit from the certification of an independent third party in order to demonstrate the compliance of their data-processing operations. Garante per la protezione dei dati personali (Italian data protection Authority), *FAQ in materia di certificazione e accreditamento ai sensi del GDPR*, available at www.garanteprivacy.it/regolamentoue/certificazione-e-accreditamento.

analyzed outside the specific context of blockchains. Some aspects of the GDPR (as underlined by the European Parliament itself in 2019[53]), such as data controllership and joint controllership, or the *right to be forgotten*, would require more regulatory effort (also from the Member States' legislators) in the sense of clearer rules that consider the specificities of use cases in a widespread manner. Similarly, we have seen how decisive the interpretative contribution of the Courts and the major independent European Authorities is. Greater coordination between the Authorities in clarifying the interpretation of the rules and key concepts of the GDPR would be auspicious.

[53] European Parliament - Panel for the Future of Science and Technology in the context of European Parliamentary Research Service (EPRS), *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, July 2019, 101.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 185-192
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 15

*Personal Data Protection in Practice of Remote Teaching in Polish Research Universities**

Jolanta Behr
(PhD and assistant professor at the Department of Administrative Law at the Faculty of Law, Administration and Economics of University of Wrocław)

Joanna Bigos
(PhD student at the Department of Administrative Law at the Faculty of Law, Administration and Economics of University of Wrocław)

ABSTRACT The article examines personal-data protection in the practice of Polish research universities. The detailed analysis concerns, i.a., legal provisions regulating this process and detailed activities undertaken by research universities towards its implementation. Emphasis is placed on implementation of the right to personal-data protection and access thereto in the context of the application of the public-interest clause. The work contains the results of research carried out at all Polish research universities and conclusions drawn on the basis of their analysis.

1. *Introduction*

Personal data protection is key for both individuals and society. For individuals, it safeguards their interest and ensures the provision of two rights: the right to personal-data protection, which is an autonomous right; and the right to privacy, which encompasses informational autonomy,[1] *i.e.*, one's right to decide on the type and extent of information that is published about them. This autonomy does also include control over this information when it is held by third parties.[2]

Society, on the other hand, benefits from-personal data protection as it ensures that public interest is pursued: unregulated, unlawful transfer of personal data leads to multiple threats to the social order and security and might lead to an increase in crime,[3] in extreme cases resulting in the loss of national sovereignty.[4]

The notion of "public interest"[5] is a general clause that refers to the use of extra-legal criteria that are individually processed by the institutions that enforce the law. The use thereof makes it possible for institutions to take a number of various actions towards personal-data protection. On the one hand, it

* Article submitted to double blind peer review.

[1] Autonomy viewed through substantive law.

[2] J. Behr, *Przyczyny ochrony danych osobowych*, in M. Błażewski and J. Behr (eds.), *Środki prawne ochrony danych osobowych*, Wrocław, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2018, 21-23. See also: M. Tzanou, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right,* in *International Data Privacy Law*, vol. 3, no. 2, 2013, 88-99; L.A. Bygrave, *Data protection pursuant to the right to privacy in human rights treaties*, in *International Journal of Law and Information Technology*, vol. 6, no. 3, 1998, 247-284; S. Rodotà, *Data Protection as a Fundamental Right*, in S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing Data Protection?*, Dordrecht, Springer, 2009, 77-82; G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, in *Law, Governance and Technology Series*, vol. 16, no. 2, 2014, 374-375.

[3] See more in M. Nawacki, *Kryminalizacja naruszenia ochrony danych osobowych*, in *Studia Prawnoustrojowe* vol. 52, 2021, 309-325; M. Brzozowska, *Kradzież danych osobowych*, in *Marketing w Praktyce*, no. 10, 2012, 87-89; P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa, Wolters Kluwer Polska, 2019, 211; I. Lipowicz, *Konstytucyjne podstawy ochrony danych osobowych*, in P. Fajgielski (ed.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin, Wydawnictwo KUL, 2008, 49; K. Sowirka, *Przestępstwo 'kradzieży tożsamości' w polskim prawie karnym*, in *Ius Novum*, vol. 10, no. 1, 2013, 64-79.

[4] M. Tzanou, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford, Hart Publishing, 2017.

[5] For more on public interest, see: A. Mednis, *Prawo do prywatności a interes publiczny*, Warszawa, Wolters Kluwer Polska, 2006; A. Żurawik, *'Interes publiczny', 'interes społeczny' i 'interes społecznie uzasadniony'. Próba dookreślenia pojęć*, in *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, vol. 75, no. 2, 2008, 57-69; E. Komierzyńska and M. Zdyb, *Klauzula interesu publicznego w działaniach administracji publicznej*, in *Annales Universitatis Mariae Curie-Skłodowska. Sectio G. Ius*, vol. 63, no. 2, 2016, 161-176; P. Górecki, *Pojęcia interes prawny i interes publiczny na tle założeń doktryny prawa*, in *Studia Administracyjne*, no. 1, 2009, 75-89.

supports personal-data protection and the right to privacy so as to ensure the well-being of the society. On the other hand, however, it allows for situations in which an institution may get involved in the sphere of rights and freedoms of the human and the citizen, provided that the law allows for such involvement. In certain legally-regulated cases, referring to the public interest makes it possible to process personal data (including sensitive data) without the knowledge and consent of the holder of those data; moreover, it results in restricting the access to the data. Hence, on a case-to-case basis, the public-interest clause does constitute a sufficient criterion for expanding or limiting the extent of the use of one's right to personal-data protection and the right to privacy.

In this context, it becomes of paramount importance that the interest evoked by the institution that processes personal data is indeed legitimate. It should be possible to account for that interest based on objective criteria[6] and data collection should be conducted in the necessary extent, time and format. Specific cases and contexts that are claimed to be conducting actions in the public interest should not simply result from current development strategies or government's policies. In these contexts, data collection would not be serving society, but rather a small, particular and elite group.

It is in the interest of those whose data are processed and gathered that the extent of data processing is as small as possible, while the processing is carried with due diligence and in compliance with legally-required procedures. Consequently, it is also important that the data be processed only by the parties who hold the consent of their holder or by the parties who have the right to process personal data based on the law.

[6] This can be validated and assessed by an appropriate court of law through a distinct procedure (see the decree of the Provincial Administrative Court of Kielce from 17 December 2020, case no. II SA/Ke 911/20, LEX no. 3115169). In some cases, public-administration bodies may evoke the notion of public interest without any justification, thereby denying a party the ability to carry out their rights and freedoms. In practice, access to public information was denied several times, which was substantiated by personal-data protection that was in the public interest. However, that protection was hypothetical rather than real, as the administrative body was using this notion to widen the gap in access to information between administration and citizens.

2. *The legal basis for processing personal data in Polish law*

Access to personal data and processing thereof requires a particular legal basis. Based on the processing party, the extent of this basis might be lesser or greater. Poland has a consolidated, baseline extent of personal-data protection, designated by state law. A large number of legal acts regulate this matter, yet there is a variance in their legal importance; they have also been issued by different entities.

The sources of law, including personal-data protection, are primarily regulated in the Constitution of the Republic of Poland of 2 April 1997[7] by the rules set off in the chapter "Sources of law".[8] These specify the sources of generally[9] and internally applicable laws. The former are applicable in the country or within the entity that created them (e.g., within a particular municipality) and may concern anyone. The latter are relevant only to the parties who are subordinate to the entity that issued them. They are therefore binding internally, within that entity, *e.g.*, within a university.

Generally applicable law, which regulates personal-data protection in the entire country is mainly based on the Constitution of Poland,[10] the Act of 10 May 2018 on Personal Data Protection[11] and Regulation 2016/679 on Protection of natural persons with regard to

[7] Journal of Laws no. 78, item 483 with later amendments; hereinafter referred to as: "The Constitution of Poland".

[8] See art. 9, 87-94 and 234 of the Constitution of Poland.

[9] In the Republic of Poland, generally-applicable law encompasses: the Constitution of Poland; international agreements that have been ratified with the prior consent expressed in a legal act; acts and statutory instruments; ratified international agreements that have not received prior consent in a legal act (the way in which ratified international agreements are constructed with or without prior legal consent are specific to Polish law. The fact that the parliament is involved in the ratification process gives the regulations specified therein primacy over other laws); and local laws and regulations. International law includes both international agreements and the legal acts of international and supernational organisations (EU). In EU law, which is a part of Polish law, these acts encompass the primary and secondary EU acts, including the founding treaties, directives, decisions (hard law), recommendations and opinions (soft law).

[10] See the overview and discussion on the most significant legal acts on personal-data protection: J. Behr, *Źródła prawa ochrony danych osobowych,* in M. Błażewski and J. Behr (eds.), *Środki prawne ochrony danych osobowych*, 42-71.

[11] Journal of Laws from 2019, item 1781.

the processing of personal data and free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).[12]

At research universities, other regulations are present beyond these acts. They are in line with generally applicable law and further delineate the rules thereof. Their goal is to adjust generally-applicable law to the conditions and peculiarities of the particular universities and their goals.

3. *Research universities: notion and meaning*

The matters pertinent to higher education in Poland are regulated by: Art. 70, section 5 of the Constitution of Poland, which introduces the notion of autonomy of the institutions of higher education;[13] and the Act of 20 July 2018 on Polish Law on Higher Education and Science,[14] which specifies the organisation and functioning of the state's higher education system.[15] That act considers universities to be the basic organisational units that carry out public actions connected to the mission of the system of science[16] and higher education.[17]

The notion of a "research university" was introduced by Art. 365, section 2, item "e" of the Law on Higher Education and Science.[18] The document established, i.a., "Excellence initiative – research university". This initiative aims to carry out the state scientific policy and the beneficiaries thereof are referred to as research universities. In legal terms, the initiative assigns additional funding[19] by the Minister of Science and Higher Education to a public[20] or non-public[21] academic university or a federation of entities that belong to higher education and science.[22] The funds are assigned based on a competition[23] and require two legal conditions to be met. In each competition, funding[24] may be attained by 10 academic universities at most.[25] The act indicates the conditions that must be met by a university for it to be able to participate in the competition.

The first competition within the initiative was announced on 26 March 2019. Out of 20 applicants, 10 winners[26] were selected:

[12] General Data Protection Regulation, *European Parliament and Council of the European Union*, L119, 4 May 2016, 1-88; hereinafter referred to as: "The GDPR".

[13] In Polish legal academic terms this is also referred to as the rule of autonomous decentralisation or administrative autonomy; see: P. Lisowski, *Podstawowe ustalenia terminologiczno-pojęciowe dotyczące organizacji prawnej administracji publicznej w ujęciu relacyjnym (dynamicznym)*, in J. Blicharz and P. Lisowski (eds.), *Prawo administracyjne, Zagadnienia ogólne i ustrojowe*, Wrocław, Wolters Kluwer Polska, 2022, 467.

[14] Journal of Laws from 2023, item 742 with later amendments.

[15] Art. 1 of the Law on Higher Education and Science.

[15] Art. 2 of the Law on Higher Education and Science holds that the mission is to teach and conduct scientific activities at the highest level, build citizenship values and participate in social growth in terms of building an innovation-based economy.

[16] The set of entities that belong to the higher-education system and science is specified by Art. 7, section 1 of the Law on Higher Education and Science.

[18] This was postulated when the Law on Higher Education and Science was being developed. H. Izdebski, *Art. 387*, in I. Izdebski and J. M. Zieliński (eds.), *Prawo o szkolnictwie wyższym i nauce. Komentarz*, II ed., Wrocław, Wolters Kluwer Polska, 2021, available at https://sip.lex.pl/#/commentary/587785703/659766/izdebski-hubert-zielinski-jan-michal-prawo-o-szkolnictwie-wyzszym-i-nauce-komentarz-wyd-ii?cm=URELATIONS (accessed on: 29.10.2022).

[19] To be used for maintenance and development of the research potential of the Polish higher-education institutions. For non-public academic institutions, funding may be used exclusively for research. For public institutions, it may also be used for didactic purposes.

[20] Art. 366, section 1, item 1 of the Law on Higher Education and Science.

[21] Art. 366, section 1, item 3 of the Law on Higher Education and Science.

[22] This possibility is indicated by Art. 173, section 5, item 3 of the Law on Higher Education and Science. When an academic university belongs to a federation, it may not participate in the competition alone.

[23] The "Excellence initiative – research university" programme involves periodically-issued competitions whose aim is to elevate the international impact of the work of Polish academic institutions. The details on the competition and the number of spots, pursuant to Art. 376 of the Law on Higher Education and Science, is announced on the website (so called *Biuletyn Informacji Publicznej*, a public information bulletin) of the Minister as an announcement that specifies the subject thereof, the entities allowed to participate, participation conditions, competition enrollment process (including appeals) and detailed assessment criteria. This excludes the use of the Act of 14 June 1960, the Administrative Procedure Code (Journal of Laws from 2023, item 775).

[24] Pursuant to the existing law, an increase in funding by no less than 10% of the funding provided in the year when the competition is announced can be retained for a 6-year period (the additional funding can be extended for additional 6 years); the regulations indicate that in the first competition, the funding is issued for 7 years due to the fact that the competition participants were to create 6-year plans for increasing the quality of scientific activity and teaching. See: Art. 305, sections 3 & 4; and Art. 389, section 3 of the Law on Higher Education and Science.

[25] See the detailed conditions: Art. 387, section 2; and Art. 388, section 2 of the Law on Higher Education and Science.

[26] The remaining 10 universities that participated in the competition received additional funding that amounted to 2% of the funding they were granted in 2019 pursuant

University of Warsaw, Gdańsk University of Technology, AGH University, Warsaw University of Technology, Adam Mickiewicz University, Jagiellonian University, Medical University of Gdańsk, Silesian University of Technology, University of Wrocław and Nicolaus Copernicus University.

The research-university status is granted to the best universities in the country that meet legally designated criteria in terms of staff quality and their achievements, as well as the quality of scientific activity and the education. The status provides increased state funding and is awarded for a limited time.

4. *Personal-data protection practices at research universities during distance learning*

The analysis of personal-data protection practices by the Polish research universities during the distance-learning period is based on the data obtained from those universities based on the information that was made available to the public.[27]

It mainly concerned the internal regulations and the legal practices of personal-data protection during the SARS-CoV-2 pandemic from 20 March 2020 to 15 May 2022.

All the research universities were requested to answer the same set of questions through a legally-formalised procedure based on a public-information request. There were 14 questions in total, divided into two sections. The first section contained four questions on the normative acts that regulated personal-data protection during the SARS-CoV-2 pandemic. The second section contained 10 questions and revolved around practical issues, including the number and the type of personal-data violations during that period; as well as the actions undertaken as a result in order to prevent the negative consequences of these violations. This section did also formulate questions related to the measures undertaken by the research universities so as to eliminate this kind of violations in the future.

The first section was mostly concerned with: the legal bases that regulate distance learning at particular universities (including the period, form and method); the regulations in terms of protecting private and work equipment used for distance learning; the communication channels available in distance learning; and the procedures to be followed in the case of violation of personal-data security of students and staff of research universities during distance learning. In particular, this component sought to discover the legal-determining factors for personal-data protection, *i.e.*, the sources of this law in terms of generally and internally-applicable law and unorganized legal sources, such as knowledge norms, good practices and habits.

The second section explored the methods of protecting the informational autonomy of students and employees during distant learning. The study examined, *i.a.*, the preparation of the research-university staff to properly follow the personal-data protection rules during distance learning, the source of data that were the basis to permit the particular students to participate in distance learning and electronic forms of confirming class attendance and verifying knowledge. Moreover, the section also inquired whether the universities conducted a threat analysis in terms of the communication tools used in distance learning. The efficiency of methods used was also examined; its goal was to establish if they provided personal-data protection, or whether certain security breaches did occur and if appropriate procedures of reporting the GDPR breaches were utilised.

Based on the responses, and given the normative acts that regulated distance learning at research universities, it was established that it was mainly generally-applicable law that was utilised, such as: the Constitution of Poland, the GDPR, the Act of 10 May 2018 on Personal Data Protection and the Act of 2 March 2020 on Special Solutions to Preventing, Counteracting and Combating COVID-19 and Other Infectious Diseases and Crisis Situations Caused by Them.[28] Moreover, legal acts that were the resolutions of the Minister of Science and Higher Education issued based on Art. 51a of the Law on Higher Education and Science were used; based on this law, under extraordinary

to Art. 380 of the Law on Higher Education and Science.

[27] Pursuant to Art. 1, section 1 of the Act of 6 September 2001 on Access to Public Information (Journal of Laws from 2022, item 902), the procedure specified therein makes it possible to file a request to public administration for information that pertains to public matters.

[28] In particular Art. 3 of the Act. Journal of Laws from 2023, item 1327 as amended.

circumstances that put the life or well-being of the members of the academic community in peril, the Minister may temporarily limit or put to halt the operations of universities within the country or its part given the level of the threat in a given area. The resolutions issued based on this law dictated that distance learning methods and techniques were to be applied to conducting courses online, regardless of whether the curriculum[29] had accounted for such possibility; this affected regular university courses, post-graduate studies and doctoral programmes and other forms of education that were conducted at universities and at other entities that were under the Minister's authority.

Outside of the generally-applicable law, to a certain extent, the issues of distance learning were also regulated by many normative acts and certain other legal acts and administrative acts issued by the university bodies and their assisting bodies, *e.g.*, through: rector's resolutions, vice-rector's resolutions, rector's announcements, university chancellor's announcements, vice-rector's announcements, announcements of rector's proxies, rector's decisions, vice-rector's decisions and rector's circulars, as well as the university senate's resolutions. All the normative acts undertaken by the university bodies and their assisting bodies were published on their respective websites under separate sections.

The analysis of the research-university responses indicates that even prior to the pandemic, the universities were indeed ensuring proper security of their staff's work and private equipment that was used for distance learning. Alongside the legal regulations, good practices and guidelines were also formulated in this regard.

Only one out of the ten research universities indicated that it had an internal regulation that specified the safety policy within its computer network. The responses did also specify that a comprehensive solution was in place at the universities, i.e., the System for Information Security Management.

Beyond the legal regulations, university staff was also obligated to participate in trainings towards personal-data protection and teleinformatic security; those who processed personal information were also required to hold special personal credentials (internal certificates for data processing).

In the context of the regulations, a question inquired whether the universities permitted any available communication channel for distance learning. Some of the universities had recommendations for a particular environment and services, while some enumerated the allowed tools (in both cases those were environments and tools available for commercial use). In most of the cases, the communication between lecturers and students (outside of class) was based on internal-communication channels that are managed and secured by appropriate organizational units within the universities. When multiple communication channels were allowed, it was specified that these were only to be used under the condition that appropriate standards were in place for the identification and security of the transferred data. In this regard, secure solutions were promoted, matching the legal requirements in place.

In this section, the public universities indicated that their internal regulations specified the appropriate reactions (procedures, guidelines) to the instances of personal-data security violations during distance learning.

The second section of the request was related to the violations of the personal-data protection law, the actions undertaken to eliminate the violations and the outcomes of the potential violations related to distance learning during the SARS-CoV-2 pandemic.

The universities did not respond to the

[29] Regulation of the Minister of Science and Higher Education of 11 March 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 405), Regulation of the Minister of Science and Higher Education of 23 March 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 511 as amended), Regulation of the Minister of Science and Higher Education of 21 May 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 911), Regulation of the Minister of Science and Higher Education of 16 October 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 1835) and Regulation of the Minister of Science and Higher Education of 25 February 2021 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 363), which was then waived on 10 August 2021.

questions in this section in a uniform fashion. It should be noted that answering the questions in a public-information request is obligatory as long as the matters of the inquiry pertain to public issues and are not in conflict with the public interest specified in the Introduction to this article. The response to the request itself is therefore legally regulated: the law specifies the required legal form of the response to the request and the allowed amount of time providing such response can take. Through an inquiry, a public administration does also establish whether responding to the request to the required extent might infringe on public interest, or whether it is without prejudice to the legally-protected data, secrets or security matters.

In most of the cases, the responses to the detailed questions were deemed to not constitute public information in the understanding of the Polish law and therefore did not need to be made available. That approach pertained to, *i.a.*: threat analysis and the notion of not conducting such analyses in terms of using new tools or systems; the approaches to personal-data security with the use of commercial tools and software, especially in the context of these data becoming available to unauthorised parties and the possibility of the data being damaged, modified or lost; information as to whether any incidents occurred or were reported at the university (incident is understood as an event in which integrity, confidentiality or availability of data might have been compromised, including the events which might carry negative consequences for the affected parties[30]), especially when staff and students were allowed to use their private inboxes to carry out actions related to the teaching process. The responses also clearly stated that information regarding IT systems, technical and organisational matters and the data on the incidents were the part of the documentation concerning personal-data protection at the university; that documentation was considered technical. It was argued that disclosing the data that constituted the university's internal documentation would compromise the security of information and loss of personal data, while publishing those data could lead to divulging information that could significantly affect, *i.a.*, the security of particular IT tools. As a result, it was deemed that the requested information that was technical at its core did not constitute public information.[31] The internal documents related to dealing with incidents were approached accordingly.[32]

In several cases, universities demanded that the petitioner (*i.e.*, the researchers conducting this study) justify the existence of the public interest that would validate the response from the research universities to the particular questions from the request for access to public information. The justification provided in the request was deemed insufficient to legitimise the existence of public interest. The authors justified the request as follows: a) the datapoints would be analysed alongside their counterparts from all other research universities towards establishing whether a systemic, coherent approach to personal-data protection existed during distance learning at these universities; b) the acquired data would make it possible to verify whether research universities, as public institutions, would be sufficiently protected against unlawful, unauthorized breaches of the integrity of their systems and data that they held; and c) the goal of the request was to ensure and improve the security of public interest. Withholding responses to many of the questions related to the important issues of personal-data protection and informational autonomy of an individual was thereby barred by the respondents.

The variety in the stances taken towards providing requested information on personal-data protection during distance learning is also apparent in the responses provided by some of the research universities. Those are very fragmented, fail to refer to the contents of the questions (in one of the cases, a response to all the questions consisted of five sentences total), and some of them respond to questions without providing any relevant justification whatsoever as to why the response does not encompass the entirety of the question asked. In some instances, the respondents deemed that some data did not constitute public information in the understanding of Polish law; therefore, that data were outside the scope of public interest. These actions are in conflict with common practices and existing legal requirements.

[30] Source: https://gdpr.pl/artykuly/co-to-jest-incydent.

[31] Decree of the Supreme Administrative Court of 16 March 2021, case no. III OSK 35/21.

[32] Decree of the Provincial Administrative Court of 7 July 2021, case no. II SAB/Go 77/21.

What is more, only one of the ten research universities responded to all the questions posed in the request. The answers were comprehensive, descriptive and precise. In this particular instance, no claims were made that the requested information did not constitute public information, and neither was any further justification required.

This diverse approach to responding to the questions means that it is not possible to formulate generalised conclusions that would account for personal-data protection applied in distance learning.

More importantly, however, this highlights an important issue, posing the question whether the public-interest clause in the context of personal-data protection is actually respected by Polish research universities. The diverse approach to responding to the request, as well as the form of the responses, suggest that safeguarding the public interest means that in some cases access to vital information is being restricted; in this case, it was impossible to use an administrative procedure[33] to access the data regarding whether and how personal data were protected during the pandemic. These practices do indeed limit the informational autonomy of an individual, with the public-interest clause being interpreted *ad hoc* and in an inconsistent manner, which is indicative of the risk of the instrumental use thereof. This practice does also cast doubt on the intentions of particular research universities. It is therefore impossible to establish whether their refusal to respond is indeed caused by justifying the existence of public interest or the failure to justify it, that being limited by the need of processing a significant amount of data that were not in the possession of the university when the request was filed, which would involve investing significant means and effort towards preparing the information; or whether it is used as basis to avoid answering the specific questions which would result in negative assessment of the practices applied at the universities, especially in the context of detecting and mitigating the results of the breaches in personal-data protection. This approach does also give rise to the question whether the incorrectly interpreted public-interest clause, with that interpretation being outside of the jurisdiction of administrative inquiry, does not widen the information gap between administrative bodies and the individual; and whether this does not create a tool that, when used with ill intent, may support the institutions in pursuing their own interests irrespectively of the rights and freedoms of an individual.

5. *Conclusions*

This article shows that Polish research universities have a wide array of normative acts and other legal acts that regulate the rules of personal-data protection in distance learning. This system appears to be comprehensive and sufficient as it is regulated by both generally-applicable law provided by the state and the executive acts that are issued by the supervisory bodies of the research universities. This is further supplemented by the acts issued by the university bodies and their assisting bodies.

The aim of the regulations issued during the pandemic was to reinforce and specify the existing solutions. The obligatory staff trainings in personal-data protection and teleinformatic security[34] are also praiseworthy, with the universities incorporating a variety of informational instruments and facilitating individual inquiries by creating dedicated websites.

To reach the aim of this article, a particular approach was taken, *i.e.*, filing a request for public-information access. There were risks bound to this approach, as access to relevant information is limited by the scope of the response of a given institution to the request itself. Insufficiently-detailed responses made it difficult to comprehensively assess the practical dimension of personal-data protection during distance learning at Polish research universities. One of the key rationales given by the universities when they partly denied access to information was the protection of public interest and retaining the security of their IT systems and the safety measures thereof. These practices seem reasonable and are backed by the stance taken by the President of the Personal Data Protection Office, that Office being the central public-administration body for personal-data protection pursuant to the GDPR. It is also in line with the decisions of the Polish administrative courts.

[33] This can be subject to an administrative court-inspection.

[34] In this case, it was also specified that the training does include the students.

There are, however, reasonable doubts bound to the discrepancies in the extent of the data that were made available. Each institution had a different understanding of what public information and the public interest clause were. This led to inconsistent practices in information access and the denial thereof. In some cases, the public-information clause was found to have restricted the informational autonomy of the university. This made it impossible to verify whether and to what extent personal data were being protected, whether they may have been exposed to breaches of their integrity, confidentiality and availability, and whether these resulted in negative consequences incurred by a given institution.

Moreover, examining the practices carried out by some of the research universities might be indicative of another worrying phenomenon. Once the requests for public-information access were issued for the purposes of this study, a shift was found in the practices related to personal-data protection. For some universities, changes were made to their internally-issued regulations for personal-data protection in the area pertaining to the issued request. Certain systems and procedures were tightened up, which does deserve approval. It is, however, debatable whether the denial of information access was truly motivated by safety concerns or whether it was dictated by the deliberate intent not to disclose the errors made by particular institutions.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 193-197
ISSN 2724-5969 – ISBN 979-12-218-0798-1 - 10.53136/9791221807981 16

*Spatial-Data Processing in the Infrastructure for Spatial Information: The Example of Poland**

Maciej Błażewski
(PhD, Faculty of Law, Administration and Economics; University of Wrocław)

ABSTRACT The infrastructure for spatial information enables the optimal use of data for space management by public-administration authorities and private entities. Spatial data relate directly or indirectly to a specific location or geographical area.
The paper focuses on analysing two levels of spatial-data processing: the organisational and technological levels. The organisational level relates to the structure of entities like public-administration authorities and private entities who process spatial data. The technological level relates to the technical standards required by electronic public registers.
The article introduces a distinction between two spheres of data processing: the sphere of open access and the sphere of limited access. The sphere of open access is basic in nature with universal and free-of-charge processing of spatial data. The limited-access sphere preserves the natural monopoly of the state in providing spatial data from public resources.

1. *Introduction*

Public-administration authorities carry out public tasks with the use of spatial data, which have direct or indirect reference to a specific location or geographical area. Spatial-data sets are contained in public registers kept by various public-administration authorities. The infrastructure for spatial information enables the optimal use of this kind of data for spatial management at the level of the European Union, member states, regions or communities.[1] The provisions of law regulating the infrastructure for spatial information have been adopted at the European-Union and national levels. Legal provisions at the European-Union level include Directive 2007/2 / EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).[2] The aim of the Directive is to ensure that the infrastructure for spatial information created by the Member States is compatible and usable in the European Community and transboundary context.[3] National regulations are contained, *inter alia*, in the Act on the Infrastructure for Spatial Information of 4 March 2010[4] and in the Land Surveying and Cartographic Law Act of 17 May 1989.[5] These levels are interrelated because of implementation of the INSPIRE Directive into national law.

The infrastructure for spatial information includes spatial-data sets and related services, technical measures, processes and procedures. This infrastructure is created mainly by public-administration authorities but it can also be created by third parties.[6] The spatial data, which are part of this infrastructure, could be processed by the public-administration authorities and third parties who created the infrastructure, as well as the users of the infrastructure.

Researching the issues of spatial-data processing requires analysing two levels: the organisational level and the technological level. The organisational level relates to the structure of the entities which form the infrastructure, and the technological level relates to the applicable technical standards. Both levels determine the method used for spatial-data processing.

*Article submitted to blind double peer review.

[1] J. Gaździcki, *Kataster nieruchomości na tle infrastruktury informacji przestrzennej*, in *Polskie Towarzystwo Informacji Przestrzennej. Roczniki Geomatyki*, Vol. 14, Issue 3, 2016, 296.

[2] Official Journal of the European Union L 108, 25 April 2007, 1-14 with amendments.

[3] Recital 5 sentence 2 INSPIRE Directive.

[4] The Act on Infrastructure for Spatial Information of 4 March 2010 (consolidated text Journal of Laws 2021, item 214), hereinafter ISI.

[5] Land Surveying and Cartographic Law Act of 17 May 1989 (consolidated text Journal of Laws 2021, item 1990 with amendments), hereinafter LSCL.

[6] Art. 3 point 2 ISI. According to art. 3 point 1 INSPIRE Directive, infrastructure for spatial information includes metadata, spatial-data sets and spatial-data services; network services and technologies; agreements on sharing, access and use; and coordination and monitoring mechanisms, processes and procedures.

2. *The organisational level*

The organisational level of spatial-information processing is based on the existing structure of the public administration. This level is governed solely by the provisions of national law, because of the institutional autonomy of Member States. The Act on Infrastructure for Spatial Information introduced a model based on existing public-administration authorities due to the need to account for various information resources.

This model includes four types of entities: the coordinator, the leading authority, the authority keeping a public register and the user. The aim of this model is to ensure effective cooperation among the public-administration authorities who create the infrastructure for spatial information.

The coordinator of infrastructure for spatial information is the Minister of Construction, Spatial Planning and Housing.[7] The Minister exercises the function with the assistance of the Surveyor General.[8] The subject of coordination includes: the creation, maintenance and development of the infrastructure for spatial information.[9]

The supreme public-administration bodies or central public-administration bodies could enjoy the status of leading authorities.[10] These authorities organise, coordinate and monitor activities to ensure the operation of the infrastructure for spatial information. The Act on the infrastructure for spatial information introduced more than one leading authority. Each of them acts according to their substantive jurisdiction.[11]

The authorities keeping public registers are stakeholders of the infrastructure for spatial information. If their public registers are related to topics of spatial data, these authorities are required to establish and maintain the network of spatial-data related services.[12] They keep public registers as required by relevant specific provisions.

The users are public-administration authorities as well as private entities that use spatial-information resources. A public administration authority who is a member of this group may, at the same time, be either the creator and user of these resources, or only a user.[13]

3. *The technological level*

The infrastructure for spatial information was created on the basis of existing public registers in which public-administration authorities and other public entities had been collecting spatial data for decades. The structure of this infrastructure allows for a more optimal use of spatial-information resources by public-administration authorities. For this reason, regulations governing the infrastructure for spatial information introduced the requirement to modernise existing public registers in compliance with technical standards enabling cooperation with other public registers.[14]

The modernisation relates to the tele-information systems, which ensure the operation of public registers. Regulations governing the infrastructure for spatial information establish some technical standards applicable to these systems. The technical standards must be harmonised according to the interoperability standard.[15] The requirement of harmonisation is fulfilled by interoperable public registers.[16]

[7] Art. 18 item 1 ISI.

[8] Art. 19 item 1 in connection with art. 18 ISI M. Baranowski, *Infrastruktura informacji przestrzennej w ujęciu systemowym*, Warszawa, Instytut Geodezji i Kartografii, 2012, 31-32.

[9] According to art. 17 item 1 ISI leading authorities, other authorities of public administration and third parties, alone as well as in cooperation with each other, create, maintain and develop the infrastructure for spatial information. According to art. 18 item 1 ISI, Minister of Construction, Spatial Planning and Housing coordinates the creation, maintenance and development of the infrastructure of spatial information.

[10] Art. 3 point 7 ISI.

[11] Art. 20 item 1 ISI.

[12] Art. 9 item 1 ISI.

[13] M. Baranowski, *Infrastruktura informacji przestrzennej w ujęciu systemowym*, 36.

[14] J. Gaździcki emphasizes that, in Poland, the infrastructure of spatial information was based on the existing technical infrastructure including public registers and other information resources. The amendments in the law mainly concerned the modernization of the existing technical infrastructure. J. Gaździcki, *Infrastruktura informacji przestrzennej w świetle doświadczeń wdrożeniowych w Polsce*, in *Polskie Towarzystwo Informacji Przestrzennej. Roczniki Geomatyki*, Vol 11, Issue 3, 2013, 10. See also J. Gaździcki, *Kataster nieruchomości na tle infrastruktury informacji przestrzennej*, 2016, 297.

[15] According to M. Baranowski, tele-information systems may achieve interoperability thanks to harmonization initiatives. M. Baranowski, *Infrastruktura informacji przestrzennej w ujęciu systemowym*, 38-39.

[16] According to art. 13 item 1 the Act of 17 February 2005 on the computerisation of entities performing public tasks (consolidated text Journal of Laws 2021, item 2070 with amendments), hereinafter CEPPT, public tele-information systems should be compatible with the minimum requirements of system interoperability speci-

Interoperability is a characteristic feature of tele-information systems and is defined as the ability to communicate with other tele-information systems without direct human interference.[17]

There are four basic layers of interoperability: 1) the organisational layer (including procedures for cooperation and procedures for informing on the method for using the tele-information systems); 2) the semantic layer (including data exchange and their correct interpretation); 3) the technological layer (relating to the structural and operational aspects of the tele-information system, as well as the syntactic aspect related to data transferring and downloading); 4) the legal layer (including legal provisions, which govern deployment of the three previous layers).[18]

The provisions of the Act on the infrastructure for spatial information require interoperability of the tele-information systems, which are part of this infrastructure. The requirements of interoperability are related to interconnection of spatial-data sets as well as the automatic interaction of spatial-data services. To meet these requirements, the leading authority should provide public administration-authorities and third parties who participate in the infrastructure for spatial information, the information required to achieve interoperability.[19] The requirement of interoperability applies to the Geoportal as well as to public registers.[20]

4. *The Geoportal*

The Geoportal is the main tool providing access to spatial-data services. It is an Internet-service operated at Geoportal.gov.pl. The Geoportal is a central access point to spatial-data services.[21] Therefore, it is the central system of the national infrastructure for spatial information as well as part of the European network INSPIRE.[22] The Surveyor General has created and maintains the Geoportal as the tele-information system allowing access to these services by means of electronic communication.[23] The Geoportal consists of two parts – the first one is a map service, and the second one is a catalogue and metadata search engine.[24] The Geoportal enables optimal sharing of spatial data with the users of this tele-information system. The Geoportal makes available spatial data previously collected in public registers, meaning spatial-data sets kept by public-administration authorities.[25]

These public registers are, inter alia: 1) the National Register of Basic Geodetic, Gravimetric and Magnetic Networks; 2) the Land and Building Register (Cadastre of Real Estate); 3) the Geodetic Register of Utilities Network; 4) the National Register of Boundaries; 5) the National Register of Geographical Names; 6) the Register of Towns, Streets and Addresses; 7) the Register of Prices of Real Estates; 8) the Topographic-Objects Database; 9) the Database of General Geographic Objects; 10) the Detailed-Control Network Database; 11) the Database of Aerial and Satellite Imagery, and Orthophotomaps and Numerical Terrain Model.[26] Spatial-data sets are also created for spatial planning, such as: 1) regional spatial development plans; 2) study of conditions and directions of spatial development of municipalities; 3) local spatial development plans (zoning plans); 4) local reconstruction plans; 5) local revitalization plans.[27] The public-administration authorities

fied in the National Interoperability Framework.

[17] M. Błażewski, *Zapewnienie interoperacyjności i systemów teleinformatycznych. Studium administracyjnoprawne*, Warszawa, Difin, 2020, 57.

[18] M. Błażewski, *Zapewnienie interoperacyjności i systemów teleinformatycznych. Studium administracyjnoprawne*, 63- 67; M. Baranowski, Infrastruktura informacji przestrzennej w ujęciu systemowym, 29.

[19] Art. 8 ISI.

[20] Paweł Sudra, *Serwis internetowy geoportal.gov.pl jako narzędzie wspomagające warsztat urbanisty*, in *Człowiek i Środowisko*, Vol. 36, 2012, 9. According to art. 13 item 1 CEPPT, public registers operating with the use of a public tele-information system should be compatible with the minimum requirements of systems interoperability specified in the National Interoperability Framework.

[21] Art. 13 item 1 ISI P. Pokojska and W. Pokojski, Geoportal krajowy ważnym źródłem *informacji przestrzennej o środowisku geograficznym w procesie edukacji*, in *Edukacja biologiczna i środowiskowa*, Vol 1, 2013, 44.

[22] P. Sudra, *Serwis internetowy geoportal.gov.pl jako narzędzie wspomagające warsztat urbanisty*, 9.

[23] Art. 13 item 1 ISI P. Sudra, *Serwis internetowy geoportal.gov.pl jako narzędzie wspomagające warsztat urbanisty*, 5; P. Pokojska and W. Pokojski, *Geoportal krajowy ważnym źródłem informacji przestrzennej o środowisku geograficznym w procesie edukacji*, 44.

[24] P. Sudra, *Serwis internetowy geoportal.gov.pl jako narzędzie wspomagające warsztat urbanisty*, 10.

[25] P. Sudra, *Serwis internetowy geoportal.gov.pl jako narzędzie wspomagające warsztat urbanisty*, 9.

[26] Art. 4 item 1a LSCL.

[27] Art. 67a item 1-2 the Act of 27 March 2003 on land planning and spatial development (consolidated text Journal of Laws 2022, item 503 with amendments).

keeping these public registers and data sets are required to keep them updated and ensure their compliance with the interoperability requirements.[28]

5. *The scope of spatial-data processing*

The processing of spatial data involves the use of these data in the infrastructure for spatial information. Spatial data are also public information.[29] The processing of spatial data is carried out using spatial-data services, which include, inter alia: searching, browsing, downloading and transforming spatial-data sets as well as activating other services.[30] There are two spheres of processing of these data: the sphere of open access and the sphere of limited access to spatial data.

The sphere of open access applies to a significant portion of spatial data. Legal regulations set out the scope of the sphere in a complex manner.

Firstly, these regulations ensure open (universal and free) access. Users of the infrastructure of the spatial information may search for data also for commercial purposes.[31] However, special regulations exclude open access for spatial-data searching. The exclusion applies to the National Geodetic and Cartographic Resource. Public-administration authorities, who maintain this resource, provide access to such materials for a fee.[32]

Secondly, the sphere of open access may be governed by specific provisions, which apply to public registers. Public-administration authorities, who keep these registers, ensure open access to data sets according to their competences.[33]

The sphere of limited access is defined by the purpose of access to spatial data. There are two levels of restrictions: 1) sharing related to performing a public task or personal use, with the exception of use for commercial purposes;[34] 2) sharing for any purpose for a fee.[35]

The second level of limitation of sharing of spatial data does not apply to the public-administration authorities and private entities that use spatial information in carrying out a public task.[36]

The purpose of limiting access to spatial data is to ensure an effective state monopoly in providing these data from public resources.[37] This limitation prevents the creation a parallel portal based on public spatial-data resources by private entrepreneurs.

The Act on the infrastructure for spatial information introduces other exceptions to sharing spatial data, which apply to 1) the implementation of international agreements binding the Republic of Poland; 2) state security; 3) public safety; 4) the activities of

[28] Art. 4 item 1d LSCL.

[29] According to art. 1 item 1 the Act of 6 September 2001 on access to public information (consolidated text Journal of Laws 2022, item 902), any information about public matters has public-information status.

[30] Art. 9 item 1 ISI.

[31] Art. 12 item 2 in connection with *a contrario* art. 9 item 2 ISI.

[32] Art. 40a item 1 LSCL. Judgment of the Regional Administrative Court in Kraków of 8 February 2017, III SA/ Kr 1304/16, CBOSA. The judgment concerns the refusal to allow free access to principal maps with electronic means of communication.

[33] The open access to spatial data, which is without fee, concerns public registers, like: 1) The National Register of Basic Geodetic, Gravimetric and Magnetic Networks (art. 40a item 2 point 1 letter f LSCL); 2) the National Register of Boundaries (art. 40a item 2 point 1 letter a LSCL); 3) the National Register of Geographical Names (art. 40a item 2 point 1 letter b LSCL); 4) the Topographic Objects Database (art. 40a item 2 point 1 letter h LSCL); 5) the Database of General Geographic Objects (art. 40a item 2 point 1 letter c LSCL); 6) The Detailed Control Network Database (art. 40a item 2 point 1 letter g LSCL); 7) the Database of Orthophotomaps and Numerical Terrain Model (art. 40a item 2 point 1 letter d as well as art. 40a item 2 point 1 letter e LSCL).

[34] According to interpretation *a contrario* art. 12 item 2 in connection with art. 9 item 1 point 1 oraz 3-5 ISI, spatial data are available through spatial-data services such as: searching, browsing, downloading and transforming spatial data sets as well as other activating services. Access to these spatial data may have a form that prevents their re-use for commercial purposes.

[35] According to art. 12 item 4 in connection with art. 9 item 1 point 3-5 ISI, public-administration authorities who are maintaining public registers, may charge fees to provide data from these registers. Fees may consider spatial-data services like downloading, transforming and other activating services. Fees are charged according to specific provisions.

[36] According to art. 14 item 1 ISI, spatial-data sets and spatial-data services, which are maintained by public-administration authorities, are available without any fee, for the performance of public tasks by other authorities and entities. According to art. 15 item 1 CEPPT, public-administration authorities and private entities who are performing public tasks have access to data collected in electronic public registers for the execution of their public tasks.

[37] Judgment of the Supreme Administrative Court in Warszawa of 11 March 2021 r., I OSK 4090/18, CBOSA. The judgment of the court concerned an administrative penalty for unlawfully using geodesy and cartography resources. The issue of the purpose of limiting access to spatial data is one of the aspects of this judgment.

the judiciary.[38]

6. *Conclusions*

In accordance with Polish law, the processing of spatial data involves the use of these data in the infrastructure for spatial information. The processing methods depend on the organisational structure of the public-administration authorities and third parties who created the infrastructure, as well as the required technical standards. This processing involves spatial data, which are directly or indirectly related to a specific location or geographical area. In principle, the processing of spatial data is universal and free of charge. The access is restricted by law because of the processing method, as well as the purpose of using spatial data. The purpose of such restrictions on spatial-data processing is to preserve the natural monopoly of the public administration, while taking into account the needs of private parties to use spatial data for their activities.

[38] Art. 16 ISI.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 199-206
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 17

*Compensation for Illegal Processing of Personal Data from the Perspective of Polish Law**

Małgorzata Kozłowska
(Research Fellow at the Institute of Administrative Sciences, Department of Administrative Law, Wrocław University)

ABSTRACT The provisions of the Polish Data Protection Act supplement Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) to the extent that this act does not regulate the issue of compensation claims for unlawful processing of personal data. After a vigorous discussion that took place in the doctrine of civil law, it was concluded that the liability for damages referred to in Article 82 of the Regulation is in tort. This determination provoked far-reaching legal consequences, since the regime of liability for damages was based in Polish law on the principle of fault. For unlawful processing of personal data, the injured party may seek compensation for material damage or compensation for non-pecuniary damage. In addition to the liability for damages specified in Article 82 of the Regulation, the EU legislator has introduced administrative-legal liability for unlawful processing of personal data. On the basis of this liability regime, Polish public entities, including public-administration bodies, can act in a dual role. On the one hand, a public-administration body may be the entity responsible for the unlawful processing of personal data and will be subject to administrative-law sanctions, while on the other hand, it may be the entity that supervises public and private entities regarding the correctness of personal-data processing.

1. *Personal-data protection in Polish law: an introduction*

Issues of personal-data protection were first regulated in Polish law in 1997, in Article 51 of the Constitution of the Republic of Poland of 2 April 1997[1] (Constitution). Article 51 of the Constitution stipulates the right to the protection of personal data, which is one of the manifestations of the right to privacy. It regulates several important issues, namely an individual's information autonomy, i.e. their freedom to provide information concerning them, the permissibility of interference with this freedom by public authorities, and their rights in the event of its infringement.[2] According to the wording of the mentioned regulation, no one may be obliged other than under the law to disclose information concerning their person.[3]

Under the Constitution, the rules and procedures for collecting and sharing personal data are determined by law. At present, it is the Personal Data Protection Act of 10 May 2018[4] (PDPA). The PDPA applies to the protection of individuals regarding the processing of personal data within the scope of article 2 and article 3 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)[5] (Regulation). The law specifies, among other things, the competent authority for personal-data protection, proceedings for infringement of personal-data protection regulations, control of compliance with

* Article submitted to double blind peer review.

[1] In *Journal of Laws*,1997, No. 78, item 483.

[2] Article 51 (Right to protection of personal data) of the Constitution:
- No one may be obliged, except on the basis of statute, to disclose information concerning their person.
- Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law.
- Everyone shall have a right of access to official documents and data collections concerning themselves. Limitations upon such rights may be established by statute.
- Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.
- Principles and procedures for collection of and access to information shall be specified by statute.

[3] M. Florczak-Wątor, *Art. 51. [Prawo do ochrony danych osobowych]*, in P. Tuleja (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa, Wolters Kluwer Polska, 2023, 190.

[4] In *Journal of Laws*, 2019, item 1781.

[5] In order to implement the PDPA, seven implementing acts and fifty amending acts have been issued in Poland and are in force in law.

personal-data protection regulations, as well as (of relevance to this article) civil liability for infringement of personal-data protection regulations and proceedings before the courts.[6]

It is worth noting at this point that the PDPA is a national supplement to the EU's Regulation. The Regulation, in accordance with Article 288 of the Treaty on the Functioning of the European Union, is of general application, binding in its entirety and directly applicable in all EU member states. To the extent that the EU legislature does not have normative competence the Regulation does not regulate certain issues related to the protection of personal data. These include system issues related to the designation of the supervisory authority and procedural issues. In addition, the EU legislator left it up to the national governments to detail certain general provisions or to shape the indicated legal constructions differently. The Polish legislator took advantage of this opportunity, regulating, inter alia, the issues of defining public entities obliged to appoint a data-protection officer and the issues of liability for violations of data-protection regulations.[7]

As G. Sibiga rightly pointed out, "Member State legislation is an exception to the principle of uniform regulation of data protection in the general regulation and should not lead to the fragmentation of personal-data protection law, which, after all, was to be counteracted by the choice of the Regulation of the European Parliament and of the Council as the harmonizing act".[8] However, when considering the issue of compensation for unlawful processing of personal data from the perspective of Polish law, it is necessary to simultaneously refer to the provisions of the PDPA and the Regulation.

2. *Legal nature of a claim for compensation for damage caused by improper processing of personal data*

Article 82 of the Regulation provides for the right to compensation for damage suffered as a result of its violation. The processing of personal data may entail negative consequences for those whose data are subjected to this process. Thus, any person who has suffered property or non-property damage has the right to obtain compensation from the controller or processor for the damage suffered. Undoubtedly, compensation under the Regulation was conceived as a tool supporting the effectiveness of regulations protecting personal data. It has a preventive function, as it is intended to provide the addressees of the Regulation's norms with an appropriate degree of motivation to comply with its provisions, and consequently prevent violations. Regardless of the preventive function, compensation for infringement of the Regulation "performs, of course, the basic function of liability for damages - it serves to compensate for the harm caused to data subjects".[9]

The concept of damage should be interpreted broadly. "Thus, it is about damage to legally protected goods or interests, both material (e.g., the financial loss that a person suffered as a result of the data processing that violated the regulation) and non-material (e.g., the harm that a person suffered as a result of the unlawful disclosure of data about his or her health; violation of the sphere of privacy, good name). Property damage includes both incurred losses and lost profits, while non-property damage refers to various types of damage to nonpecuniary assets".[10]

The institution of compensation referred to in Article 82 of the Regulation is of a civil law (private law) nature and concerns the horizontal relationship between the controller or processor and the data subject. In turn, the very construction of Article 82 of the Regulation makes it possible to assume that this provision is an independent basis for compensation claims. However, since legal proceedings for damages are initiated before a court of competent jurisdiction under the law of a member state, the Polish legislator has

[6] In *Official Journal of the European Union*, 2016, item 119.

[7] P. Fajgielski, *General Data Protection Regulation. Personal Data Protection Act. Commentary*, II ed., Warszawa, Wolters Kluwer, 2022, 76.

[8] G. Sibiga, *General Data Protection Regulation. Current problems of legal protection of personal data*, Warszawa, C.H. Beck, 2016, 18.

[9] R. Strugała, *Principle of compensatory liability for damage caused by improper processing of personal data (Article 82 RODO)*, in J. Jezioro, K. Zagrobelny and K. Wesołowski (eds.), *Selected issues of Polish Private Law. A memorial book in memory of PhD Józef Kremis and PhD Jerzy Strzebińczyk*, Wrocław, EDITOR, 2019, 208.

[10] P. Fajgielski, *Komentarz do ustawy o ochronie danych osobowych*, in P. Fajgielski (ed.), *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, II ed., Warszawa, Wolters Kluwer Polska, 2022.

detailed the regulation of civil liability in Chapter 10 of the PDPA (articles 92, 93 and 100). These provisions stipulate, in particular, among other things, that to the extent not regulated by the Regulation, the provisions of the Civil Code shall apply to claims for infringement of personal-data protection regulations, the district court shall have jurisdiction over claims for infringement of personal-data protection regulations, and the provisions of the Code of Civil Procedure shall apply to proceedings to the extent not regulated by the Law.

In the doctrine of Polish civil law , due to the statutory reference to the provisions of the Civil Code to the extent that the Regulation does not regulate all issues of liability for damages for violation of the provisions on personal-data protection, a discussion has swept over whether this liability is based on the principle of fault or risk? A question was posed about the legal nature of the claim for damages, that is, is it tort or contractual in nature? Doubts arose over the Polish translation of Article 82 of the Regulation. In most, if not all, language versions of the Regulation, the wording of Article 82 predetermines that the administrator can be released from liability if they prove that they are not responsible for the event that caused the damage, while the Polish version uses the premise of no fault. Part of the doctrine of Polish civil law has advocated the concept of strict liability, arguing that it is not so much the absence of fault that should be considered an exonerating circumstance as the fact that the damage resulted from extraordinary events beyond the control of the administrator whose liability is under consideration. The reasonableness of this position was derived directly from the interpretation of the Polish version of the Regulation, where it referred to the phrase about "not being at fault for the event that led to the damage". In the end, the concept of fault-based liability prevailed, whose proponents referred directly to the wording of Article 82(3) of the Regulation. In fact, this provision stipulates that the controller or processor shall be exempted from liability if they prove that they are in no way at fault for the event that led to the damage.[11] Another argument in favor of assuming that liability for damages for violation of the Regulation is of a tort nature is that its basis is the violation of norms of a general nature, addressed to an indeterminable circle of addressees, rather than relative norms, existing between specific individuals.[12]

Determining that liability for damages under Article 82 of the Regulation is based on the principle of fault determines that in matters not regulated by the Regulation, the provisions of the Polish Civil Code on tort liability should be applied.

3. *Types of compensation claims for unlawful processing of personal data under Polish law*

The Regulation regulates the pursuit of data-breach claims in articles 79 and 82, but does not do so exhaustively. The Polish legislator has not decided to introduce a new measure into the legal system at the level of substantive law,[13] resolving, however, that the EU's data-subject claims regulations would be supplemented by the Civil Code. The reference to the provisions of the Civil Code means that the provisions of Article 415 et seq. and Article 448 et seq. of the Polish Civil Code of 23 April 1964, apply to claims for violations of data-protection regulations[14] (PCC). The norm of Article 415 of the PCC will be applied to cases claiming compensation for property damage suffered as a result of a violation of data-protection regulations, while from Article 448 of the PCC to claim compensation for non-pecuniary damage suffered.

Damage should be understood as any harm suffered against the will of the injured party in their legally-protected goods or interests.[15] The Polish legislator adopts the principle of full compensation for damage suffered for unlawful processing of personal data, regardless of whether it is of a pecuniary (on the basis of article 361 § 2 PCC[16]) or non-

[11] R. Strugała, *RODO and liability for damages. Basic problems of liability for damage caused by improper processing of personal data*, in *Legal Monitor*, vol. 17, 2018, 916-917.

[12] A. Pązik, *Damage resulting from violations of RODO. Selected issues*, in *Scientific Journals of the Jagiellonian University. Papers in Intellectual Property Law*, vol. 3, 2020, 127-146.

[13] In *Journal of Laws*, 2022, item 1360.

[14] Article 415 PCC states that: Anyone who by a fault on his part causes damage to another person is obliged to remedy it.

[15] A. Sinkiewicz, The concept and types of damage in Polish civil law, in Notary, vol. 2, 1998, 62.

[16] Article 361 PCC Causal relationship; damage.
1. A person obliged to pay compensation is liable only for normal consequences of the actions or omissions

pecuniary nature.[17] This means that, if nothing else follows from the provision of the law or the agreement between the parties, the injured party should be compensated for the full amount of the damage, and the court that decides on this compensation is under no discretion to measure it.

By the term pecuniary damage it is meant damage to property (directly conditioned by economic interest, the value of which is expressible in money). Non-pecuniary damage, on the other hand, is damage to non-material goods (it does not directly relate to the property sphere, and therefore - the value of intangible goods cannot be directly estimated in money). Damage resulting from unlawful processing of personal data can take several forms. It can be a property damage resulting directly from the infringement of goods of a pecuniary nature, a property damage resulting from the violation of goods of a non-pecuniary nature - but causing effects in the property sphere of the injured person, and a non-pecuniary damage in the form of harm, that is, relating to the mental sphere of the injured person.

Regardless of the form of damage, however, compensation claims essentially consist of the ability to demand damages (in the case of property damage) or monetary compensation for the harm suffered (in the case of non-property damage). In each case, the prerequisites for compensation will be the existence of unlawful damage, the occurrence of an event in which a provision of generally applicable law attaches liability to the debtor, a causal connection between the event and the damage, and fault.

Under Polish law, the limits of compensation for property damage are set by financial loss and lost profits. By the term financial loss (damnum emergens) is meant a decrease in assets or an increase in liabilities. Lost benefits (lucrum cessans) include the value of assets that did not become part of the estate as a result of the harmful act, and the value of liabilities that did not diminish as a result of the damage. There is a consensus that only those benefits should be taken into account, which with a high probability would be in the property of the injured party. If this probability is lower, there is a case of so-called "contingent damage" (loss of the chance to obtain benefits), which is not subject to compensation.[18] The determination of the existence and amount of damage is made by the differential method, which prescribes to take as damage the difference between the actual state of the injured party's property at the time of the determination and the hypothetical state that would have existed if the causal event had not occurred. Its characteristic feature is that it takes into account all the consequences of a specific event for the property of the injured party, so not only the direct effects on individual property, but also further consequences on the property of the injured party. On the other hand, the establishment of lucrum-cessans damages requires the demonstration in a particular case of a high degree of probability of loss of benefits, although proof of certainty of occurrence is not necessary.[19]

A claim for compensation as a form of reparation for non-pecuniary damage (harm) is available to the injured party only in cases specified by law. It provides a method of compensating for the harm resulting from the violation of personal rights. In other words, it is a matter of redressing the psychological suffering resulting from the unlawful processing of personal data.[20] This refers to non-material damage existing both at the time of the court's decision and that which the injured party will suffer in the future certainly or with a foreseeable high degree of probability. The amount of compensation depends on the totality of the circumstances of the particular case, concretizing in relation to the injured person. In the jurisprudence, an accurate view has been formed that the essential prerequisites for determining its amount are the type, nature and duration of

from which the damage arises.
2. Within the above limits, in the absence of a provision of the law or contract to the contrary, remedy of damage covers the losses which the aggrieved party has suffered, and the benefits which they could have obtained had it not suffered the damage.

[17] The provisions of Polish law stipulate compensation for non-material damage in the form of harm when a special provision governs it. In this case, the specific provision allowing compensation for non-pecuniary injury under Polish law will be Article 82(1) of the Regulation.

[18] G. Karaszewski, *Artykuł 361*, in J. Ciszewski and P. Nazaruk (eds.), *Kodeks cywilny. Komentarz aktualizowany*, LEX/el., 2022.

[19] Judgment of the Court of Appeal in Krakow from 15 July 2015 r., I ACa 483/15, LEX number 1934435.

[20] A. Szpunar, *Compensation for non-pecuniary damage*, Bydgoszcz, Oficyna Wydawnicza Branta, 2004, 164-169.

negative psychological experiences. Such indications also include the degree of guilt of the wrongdoer, the attitude of the person responsible for causing the damage, their behavior toward the injured party, in particular whether they took steps to compensate for the harm.[21]

4. *The administrative liability for unlawful processing of personal data*

In addition to the liability for damages provided for in Article 82 of the Regulation, the EU legislator has introduced administrative liability for unlawful processing of personal data. Administrative fines imposed in each member state by supervisory authorities, that is, public administrations, have been added to the catalog of sanctions for violations of the Regulation. Article 83[22] of the Regulation

[21] Judgment of the Supreme Court of 12 September 2002, IV CKN 1266/00, LEX number 80272.

[22] Article 83 [General conditions for imposing administrative fines].
1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
the intentional or negligent character of the infringement;
b) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
c) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
d) any relevant previous infringements by the controller or processor;
e) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
the categories of personal data affected by the infringement;
f) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
g) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
h) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
i) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
b) the obligations of the certification body pursuant to Articles 42 and 43;
c) the obligations of the monitoring body pursuant to Article 41(4).
5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
b) the data subjects' rights pursuant to Articles 12 to 22;
c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
d) any obligations pursuant to Member State law adopted under Chapter IX;
e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.
8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States

specifies the prerequisites for the application of an administrative fine, sets the amount of the fine and indicates the circumstances affecting it.

Considerations conducted in the science of Polish administrative law on the essence of the administrative fine as a type of administrative sanction for unlawful processing of personal data led to the introduction of a legal definition of this concept in the Polish legal order. According to Article 189b of the Polish Code of Administrative Procedure,[23] an administrative monetary penalty should be understood as a sanction of a pecuniary nature that is defined by law and is imposed by administrative decision by a public-administration body following a violation of the law consisting of a failure to comply with an obligation or a violation of a prohibition imposed on a natural person, a legal person or an organizational unit without legal personality. At the same time, it should be noted that the provisions of the Regulation are *lex specialis* in this case and take precedence over Polish administrative procedure. However, they are not complete and therefore must be augmented with selected provisions of the Polish Administrative Procedure Code and PDPA that do not contradict them.[24]

On the basis of the issue at hand, public entities, including public-administration bodies, can act in a dual role. On the one hand, the public-administration body may be the entity responsible for the unlawful processing of personal data and will be subject to administrative-law sanctions, while on the other hand, it may be the entity that exercises supervision over public and private entities in verifying the correctness of personal-data processing.

The responsible entity under the PDPA, as well as the Regulation, can be either a public entity or a private entrepreneur, as long as it is the personal data administrator. These entities are entirely responsible for the implementation of tasks and processes under data-protection laws, for their proper functioning and for the supervision of designated data-protection officers. It should be noted that the amount of administrative sanctions was determined separately for public entities and other subjects. Article 83(7) of the Regulagtion indicates that each member state may determine whether and to what extent administrative fines may be imposed on public authorities and entities established in that member state. Poland has taken advantage of this possibility by stipulating the maximum amount of administrative fines that can be imposed on public entities. The imposition of penalties on public finance-sector entities is regulated by article 102 of the PDPA. The central authority of the Polish public administration, which is the President of the Office for Personal Data Protection, may impose, by decision, administrative fines of up to PLN 100,000 - on units of the public finance sector referred to in article 9 points 1-12 and 14 of the Public Finance Act, research institutes, the National Bank of Poland, as well as fines of up to PLN 10,000 - on units of the public finance sector referred to in article 9 point 13 of the Public Finance Act.[25]

The legislator justified the differentiation of maximum penalties by the perpetrator on the grounds that public entities are financed from state-budget funds. In addition, imposing penalties on the public administration in significant amounts indirectly burdens tax-paying citizens. This position perfectly demonstrates the consciousness of the legislator in assigning a purely repressive function to administrative punishment imposed on public entities, including public-administration bodies. The justification for the introduction of lower fines that can be imposed on public entities is also that the financial administrative sanction can lead to the bankruptcy of public entities with low revenues.[26]

shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

[23] Act of 14 June 1960 Code of Administrative Procedure, Journal of Laws 2022, item 2000.

[24] J. Łuczak, *Artykuł 83 (Ogólne warunki nakładania administracyjnych kar pieniężnych)*, in E. Bielak-Jomaa and D. Lubasz (eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa, Wolters Kluwer Polska, 2018.

[25] L. Staniszewska, *Model karania za przetwarzanie danych osobowych niezgodnie z przepisami*, in M. Jędrzejczak (eds.), *Ochrona danych osobowych w prawie publicznym*, Warszawa, Wolters Kluwer Polska, 2021.

[26] However, the Polish legislator has adopted an additional repression for public entities manifested in the mandatory publication on the website of the entity or on the website of the Public Information Bulletin of the final decision stating the violation, while with regard to entrepreneurs, publication takes place only if the author-

The introduction by the Regulation of a new power for supervisory authorities to impose administrative fines for violations of data-protection regulations is one of the most significant changes in the data-protection system. In this way, the EU legislator aims to increase the effectiveness of enforcement and thus improve the level of personal-data protection in the EU.

Pursuant to Article 101 of the PDPA, the supervisory authority with the power to impose an administrative fine in the event of unlawful processing of personal data, and thus the authority with the power to impose fines, is the President of the Office for Personal Data Protection. It is the central body of Polish public administration appointed and dismissed by the Sejm of the Republic of Poland with the consent of the Senate of the Republic of Poland for a four-year term.

The President of the Data Protection Authority exercises supervisory powers over both public and private entities. To the extent that the Authority examines the correctness of the processing of personal data by controllers who are public entities, including public administration bodies, it performs public-administration control in a broad sense.

The Polish supervisory authority has the power to impose an administrative fine by way of an administrative decision, the issuance of which should be preceded by a thorough administrative procedure. In connection with pending proceedings for the imposition of an administrative monetary penalty, the entity against which the proceeding is conducted shall be obliged to provide the President of the Office for the Protection of Personal Data, at any of their requests, within 30 days of receipt of the request, with the data necessary to determine the basis for the assessment of the administrative monetary penalty.

The President of the Office for Personal Data Protection, in assessing the facts surrounding the violation and determining the amount of the fine, evaluates each case individually (Article 83(2) of the Regulation). The Authority takes into account both the circumstances of the violation itself, including the attitude of the responsible entities toward the violation, and the general circumstances of the entities' compliance with the requirements of the Regulation, including the adjustment and precautionary measures taken previously and the behavior of the entities in the face of the President's previous instructions or sanctions. In addition, the President of the Office will take into consideration the profitability of the violation for those responsible and any other relevant circumstances.

5. *Summary*

The Regulation, which has been in force since 25 May 2018, besides a number of very severe sanctions of an administrative-legal nature, also provides for compensatory (civil) liability of entities involved in the processing of personal data. Article 82(1) of the Regulation grants any person who has suffered pecuniary or non-pecuniary damage as a result of a violation of the Regulation the right to obtain compensation from the controller or other processor.

The assumption under Polish law that the claim under Article 82 of the Regulation is a tort has significant legal consequences related to the pursuit of claims for damages for unlawful processing of personal data. That is because the provisions of the PCC relating to torts will be applicable here, and in particular those relating to the issue of claiming damages, or monetary compensation for harm suffered.[27]

In the course of the trial, the burden of proof is on the injured party, who, in addition to the prerequisites for tort liability, is required to indicate the amount of damage that will entail the amount of compensation or damages awarded. However, it is worth emphasizing that the Polish legislator regulates differently the conditions for claiming compensation for pecuniary damage and for compensation for non-pecuniary damage in connection with the unlawful processing of personal data.

In parallel with civil liability, the violator faces administrative liability for infringement of personal-data processing regulations. It can be borne by both public entities, including public authorities, and private entities to the extent that they unlawfully processed personal data. The administrative fine is imposed by

ity considers that the public interest warrants it, but the decision does not require anonymization (article 73 of the PDPA).

[27] N. Zawadzka, *Artykuł 92*, in D. Lubasz (ed.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa, Wolters Kluwer Polska, 2019.

the supreme administrative body of public administration - the President of the Office for Personal Data Protection, after a thorough administrative investigation. Its amount varies and depends on whether the violator of the Regulation and the PDPA is a public or private entity. The establishment of lower administrative penalties that can be levied against a public entity is dictated by the fact that its funds come mainly from taxes, which consequently is also severe for citizens.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 207-224
ISSN 2724-5969 - ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 18

*Artificial Intelligence as a Tool to Make Better Regulations**

Elsa Marina Álvarez González
(Professor of Administrative Law, Academic Secretariat of I-INGOT, Instituto de Investigaciones Jurídicas en Gobierno y Territorio, University of Málaga)

ABSTRACT Excessive regulations constitute a serious problem and have created a weak system of legal sources made up of laws and regulations that lack quality and rationality. This deficient legislative technique undermines the principle of legal certainty and, in our opinion, contributes to the present lack of trust in the political-legislative system. Given this situation, we believe there is an urgent need to improve regulatory quality in order to ensure good governance and high levels of transparency. To achieve this, introducing artificial intelligence into the regulatory process is, in our view, essential. Although this is not yet provided for in our legal system, given the advances in technological innovations and their application to many areas of activity, including administrative action, we believe that this is an issue which administrative law must address sooner rather than later.

1. *Introduction*

The regulatory function in Spain and other neighbouring countries is being negatively affected by accelerated changes currently taking place. Excessive regulations constitute a serious problem and have created a weak system of legal sources made up of laws and regulations that lack quality and rationality. This deficient legislative technique undermines the principle of legal certainty and, in our opinion, contributes to the present lack of trust in the political-legislative system.

Given this situation, we believe there is an urgent need to improve regulatory quality in order to ensure good governance and high levels of transparency. To achieve this, introducing artificial intelligence into the regulatory process is, in our view, essential. Although this is not yet provided for in our legal system, given the advances in technological innovations and their application to many areas of activity, including administrative action, we believe that this is an issue which administrative law must address sooner rather than later.

Moreover, if artificial intelligence can be used by public administrations to streamline and speed up the processing of administrative procedures, or to issue reports generated by algorithms based on the data held by a given body, we believe that it can also be useful in the regulatory process.

Artificial intelligence can contribute to better quality decision-making based on a thorough analysis of all the data made available to the public administration, and on existing precedents. In our view, this will also contribute to improving the quality of our regulations. This would mean automating certain procedures in the regulatory process, without, of course, affecting the rights of citizens and groups who play an active role in the process, especially in the prior consultation and public information procedures.

Several public bodies are providing significant impetus to improving the quality of regulations. These include the adoption by the EU of the Recommendation of the Council of the Organisation for Economic Co-operation and Development (OECD) on improving the quality of government regulation (1995) and the 2001 White Paper on European Governance, which makes better law-making an objective. Other examples include the "Interinstitutional Agreement on Better Law-making" adopted by the European Parliament, the Council and the European Commission in December 2003, and the March 2005 action plan, "Better Regulation for Growth and Jobs in the European Union", which updates and complements the 2002 Action Plan for "Simplifying and Improving the Regulatory Environment". In addition, the document "Guiding Principles for Regulatory Quality and Better Regulation" (2005) states that regulatory quality is crucial to the effectiveness of government action, and introduces, through regulatory impact analysis, an EU-wide need to assess, structure and support political decision-making. It also requires the Commission to submit an annual report to the European Council and the

* Article submitted to double blind peer review.

European Parliament on the application of the principles of subsidiarity and proportionality and on activities to improve the quality and accessibility of legislation.

The EU's objectives are clearly laid out in the "Better Law-making 2006" report, which states that: "A regulatory environment that is well-devised, clear, understandable and as simple as possible is key to protecting citizens' welfare, public health and the environment. At the same time it ensures a fair market place where European business can compete effectively and with innovative products. The Better Regulation agenda sets out to achieve this at both EU and national level in a concerted effort by EU institutions and Member States and in a manner that maximises public policy benefits while minimizing the costs that regulations impose on the EU economy." It is therefore evident from this programme that a clear and simple regulatory framework is essential for society and the economy, and that this applies across the board to all public institutions.

Also noteworthy is the 2010 Communication on "Smart Regulation in the EU", which not only complements and reformulates some of the regulatory quality principles in the "Better Regulation" initiative, but also includes principles such as the ex-post evaluation of legislation and improved electronic access to all EU legislation.[1]

The 2015 "Better Regulation" agenda is a package of measures that applies both to new legislative proposals and existing European legislation. It covers the whole policy cycle which includes preparation, adoption, implementation (national transposition, delegated acts of the European Commission), application (including monitoring and effective compliance by the Member States) and evaluation and revision. In addition, any EU intervention must take into account its legal, economic and environmental impact in order to ensure sustainable development (art. 11 TFEU). Moreover, in accordance with the principles of subsidiarity and proportionality (art. 5.1 TEU), in areas of shared competence, the EU must be able to justify the added value of its action and not go beyond what is necessary to address the problem at hand at the supranational level.[2] In this regard, we can highlight the adoption of a set of guidelines designed to help Commission services improve the way they legislate throughout the regulatory cycle and to explain how the Commission helps Member States implement EU law.[3] The guidelines are complemented by a "Better Regulation" toolbox which provides detailed guidance on issues such as drafting the explanatory memorandum that the Commission must ensure accompanies legislative proposals, and the choice of the specific legal instrument or implementation plans.[4]

This new approach to European regulatory activity has the support and participation of the two institutions that make up the European legislature, namely, the Council and the European Parliament. This is evidenced by the 2016 Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on better law-making.[5]

Also noteworthy is the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Better Regulation: Joining forces to make better laws", of 29 April 2021, in which the European Commission outlines the achievements made in this area, and the issues that still need to be addressed in order to achieve better law-making. Among its achievements is the "Fit for Future Platform" launched by the Commission in May 2020, and whose 2021 work programme highlights the potential of digitalisation, the need to support the efficiency of classification, authorization, and notification obligations, and improve legislative quality to avoid inconsistencies or duplication, while adopting

[1] All the measures adopted by the European Commission regarding better regulation can be found on the Better Regulation website (http://ec.europa.eu/governance/better_regulation/index_es.htm) and the Impact Assessment website. (http://ec.europa.eu/governance/impact/index_en.htm).

[2] B. Pérez De Las Heras, *La agenda de legislar mejor como eje de gobernanza democrática en la Unión Europea: impacto y potencialidades para las entidades subestatales*, in *Revista General de Derecho Administrativo*, no. 50, 2019, 3.

[3] European Commission, *Better Regulation guidelines*, Commission Staff Working Document, SWD (2017) 350, 7 July 2017, available at https://ec.europa.eu/info/sites/info/files/better-regulation-guidelines. pdf.

[4] European Commission, *Better Regulation toolbox*, available at https://ec.europa.eu/info/sites/info/files/better-regulation-toolbox_2.pdf.

[5] Published in the DOUE L 123 of May 12, 2016. This Agreement replaces the 2003 Agreement and the 2005 Interinstitutional Agreement on Impact Assessment.

a consistent forward-looking approach.

As regards Spain, the first measure taken in this area was the approval of several guidelines by the Council of Ministers. These include the Agreement of the Council of Ministers of 18 October 1991, approving the guidelines on the form and structure of draft bills,[6] and the Agreement of the Council of Ministers of 22 July 2005, approving the guidelines on regulatory technique.[7] Both provide technical guidance on the preparation and, in particular, the drafting of legal provisions. They do not confer any rights or obligations on third parties, and being non-regulatory in nature, cannot be invoked as a source of law in court. They have been adopted to facilitate the understanding and application of regulations.

In addition to these guidelines on regulatory technique, we must add some factors directly or indirectly related to the legislative technique that some laws have regulated rather unsystematically. These include the obligation to respect the principles of necessity, proportionality, legal certainty, transparency, accessibility, simplicity and effectiveness in the exercise of the regulatory initiative; the ex ante and ex post analysis of regulations and the guarantee of a public hearing during the drafting stage of regulations, which is included in Spanish Law 2/2011, of 4 March, on Sustainable Economy (hereinafter, LES). Other examples include Spanish Law 19/2013, of 9 December, on Transparency, Access to Public Information and Good Governance (hereinafter, LTAIBG), which aims to increase and strengthen transparency in public activities through active disclosure obligations for all public administrations and public entities in terms of institutional, organizational, and planning information; and Spanish Law 20/2013, of 9 December, on the Guarantee of Market Unity (hereinafter, LGUE), which aims to promote an efficient regulatory framework for economic activities that simplifies existing legislation, eliminates unnecessary regulations, establishes more streamlined procedures and minimizes administrative burdens.

However, the most significant progress in this area was the regulation of the principles of good regulation in Spanish Law 39/2015, of 1 October, on the Common Administrative Procedure for Public Administrations (hereinafter, LPAC). Title VI of this law is dedicated to the legislative initiative and regulatory power of public administrations. In addition to some improvements to current regulations on hierarchy and the publication of rules and principles of good regulation, it includes new provisions aimed at increasing citizen participation in the procedure for drafting regulations, together with new provisions on the ex ante and ex post evaluation of the impact of regulations.

Finally, a number of autonomous communities have also been innovative in these areas. These include Catalonia which has had a very active better-regulation policy for more than ten years.[8] Nevertheless, all public authorities should be aware of the importance of improving our regulations. An important step forward was the creation of the Observatory of Good Regulatory Practices by the Spanish government and the autonomous communities in December 2022, although we will have to wait until it is up and running to assess its effectiveness.

In any event, this paper has a forward-looking perspective, as it seeks to lay the foundations for what the regulatory process will be (or should be) like in the coming years. This inevitably means taking into account technological advances and the implementation of artificial intelligence in public administration in order to apply them to the regulatory process. We believe this will help improve the quality and rationality of our regulations.

2. *The Regulatory Process: Open and Electronic*

When we talk about the regulatory process, we are not just talking about the administrative process of drafting regulations (whether legal or regulatory), rather, the regulatory process encompasses all the actions that take place from the moment the public decision is taken, including the process of drafting the regulation and its period of validity, until the moment it is no longer part of the legal system.[9] Therefore, it includes

[6] Published in the BOE of 18 November 1991.
[7] Published in the BOE of 29 July, 2005.
[8] https://presidencia.gencat.cat/es/ambits_d_actuacio/millora_regulacio_normativa/.
[9] Professor D. Canals Ametller, *El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos)*, in *Revista General de Derecho Administrativo*, no. 50,

regulatory impact assessments, whether ex ante (before drafting and adoption) or ex post (after publication and implementation), as well as any amendments to the legislation before it is repealed or annulled. The regulatory cycle thus includes conception, drafting, implementation, evaluation and review.[10]

The measures adopted in recent years in Spain as regards regulatory quality and in particular the amendments made to the LPAC, have strengthened the principles of good regulation and affect the entire regulatory process. Thus, art. 129.1 LPAC establishes that the exercise of regulatory initiative by the competent administrations is subject to the principles of necessity, effectiveness, proportionality, legal certainty, transparency and efficiency. These principles address the need to bring law-making and governance closer to citizens. In this way, citizens can be involved in the process of adopting regulations that may affect their rights and interests. In short, it is a form of open government in an environment conducive to dialogue and continuous interaction, with greater emphasis on public transparency and citizen participation in the definition and implementation of public policies and the adoption of legal regulations.[11]

Open government seeks to unite two fundamental concepts of developed societies: government and citizenship. For open government to work, ensuring access to information, providing adequate channels for public participation and reinforcing transparency and accountability[12] is fundamental. This is closely linked to good governance, which is regulated by national and autonomous community transparency laws. The aim of these laws is to increase and strengthen the transparency of public activities, regulate and guarantee the right of access to information and establish the good governance obligations that public officials must comply with.[13] Accordingly, if good governance refers to the way governments and senior officials carry out their functions,[14] good administration refers to the way administrative functions are carried out, with the opposite being the concept of maladministration.[15] Both concepts are included in a number of international and national regulations.[16]

If we link the ideas of good governance and good administration to the regulatory process, it would be easy to achieve an open and transparent regulatory process that guarantees good governance. Thus, when the LTAIBG sets out the obligation to carry out public functions transparently, it is also referring to regulatory transparency and greater openness towards citizen participation in the drafting of regulations, which would lead to better regulatory output (art. 26.2).

2019, defined it as "a set of actions and stages leading to the adoption of a public decision of a regulatory nature which constitutes the lifecycle or validity of a legal regulation until it is no longer part of the legal system".

[10] F. De Montalvo Jääskeläinen, *La evaluación ex post de las normas: un análisis del nuevo modelo español*, in *Revista Parlamentaria de la Asamblea de Madrid*, no. 36, 2017, 148.

[11] The OECD defines open government as "a culture of governance that promotes the principles of transparency, integrity, accountability and stakeholder participation in support of democracy and inclusive growth." (OECD Recommendation of the Council on Open Government, of December 14, 2017).

[12] The Spanish IV Open Government Plan 2020-2024, approved on October 29 2020 by agreement of the Plenary of the Open Government Forum, includes 10 commitments made by public administrations to boost transparency and accountability, improve participation, establish public integrity systems, and raise awareness of open government among citizens and public employees, with the aim of contributing to a more just, peaceful and inclusive society.

[13] On good governance, see M. Zambonino Pulito, *Buen Gobierno y Buena Administración. Cuestiones claves*, Madrid, Iustel, 2019.

[14] See in this regard, M. Villoria Mendeta and A. Izquierdo Sánchez, *Ética pública y buen gobierno: Regenerando la democracia y luchando contra la corrupción desde el servicio público*, Madrid, Tecnos, 2015.

[15] See J. Ponce Solé and M. Villoria Mendieta, *Presentación del Anuario y Estudio introductorio a la edición de 2019: el impacto de la pandemia de COVID-19*, in *Anuario del Buen Gobierno y de la Calidad de la Regulación*, Madrid, Fundación Democracia y Gobierno Local, 2020.

[16] For instance, the Charter of Fundamental Rights of the European Union (art. 41); the EC (although it implicitly refers to good administration, as argued by J. Ponce Solé, in *Deber de buena administración y procedimiento administrativo debido. Las bases constitucionales del procedimiento administrativo y del ejercicio de la discrecionalidad*, Pamplona, Lex Nova, 2001); and the Statutes of Autonomy (which already expressly include the right to good administration). Moreover, the right to good administration is already applied on a daily basis to resolve certain disputes by the Spanish Supreme Court and the courts of justice of the autonomous communities, which have handed down many rulings on the matter. Thus, for example, in the judgement of 18 December 2019, the Supreme Court stated that "... the right to a good public administration gives rise to the effective implementation of a number of citizens' rights. It is not, therefore, merely a formula devoid of content, but instead obliges public administrations to fulfil these rights in such a way that a correlative set of enforceable duties is imposed on them ...".

Regulatory transparency should apply to the entire regulatory process and not only to public access to regulations once they have been adopted. We therefore believe that transparency should cover the processing of the regulatory dossier itself, including the preliminary phase, the process of drafting the content of the regulation and the stakeholders involved. This not only allows for a better understanding of the legal regulation, but also provides a "regulatory footprint", i.e., the ability to know which stakeholders were involved in the process of drafting the regulation. This is achieved by disclosing the contacts with the administration that promoted the regulatory initiative and indicating which of the contents of the regulation stem from the contributions of these interest groups.[17] It is also important to keep records in an administrative file. In Spain, informal meetings of executive branch officials who lobby for draft laws and regulations have not so far been made public, but the obligations of transparency and the right to good administration mean that this situation must change.[18]

In addition, the regulatory process must be an electronic process. If we want to improve the effectiveness and efficiency of the process, we must use electronic media and new information and communication technologies (ICTs).[19] Thus, art. 133.1 LPAC regulates the procedure of prior public consultation, stipulating that this procedure must be carried out through the web portal of the competent administration. Similarly, art. 133.2 LPAC stipulates that the normal hearing procedure for those whose rights and interests may be affected by the future regulation must be carried out on the corresponding web portal.[20] However, we must also encourage the use of digital platforms and social networks. Although the presence of public administrations on these platforms is still at an early stage, digital participation in the regulatory process opens the doors to numerous innovative technological possibilities, such as the use of artificial intelligence and big data in the regulatory decision-making process and in the actual drafting of the regulation. We are convinced that the correct use of digital platforms would allow us to gather empirical data that could be used to improve our regulatory quality and techniques, although we are of course aware of the risks and challenges involved.

Other countries are now using this type of technology in the regulatory process. One example is the US, where computational text analysis is being applied to the electronic regulatory process, known as eRulemaking. This is carried out on a digital platform which encourages a high level of citizen participation. In the final section of this work, we will return to these issues and discuss the benefits of using technological innovation in the regulatory process.

3. *The Use of Artificial Intelligence in the Regulatory Process*

There is no denying that artificial intelligence has become an integral part of our lives. It is already used in many areas of society (health, finance, marketing, mobility, etc.) and, of course, in public administration. The advantages of using technological tools

[17] See J. Ponce Solé, *Mejora de la regulación, lobbies y huella normativa*, Valencia, Tirant Lo Blanch, 2016.

[18] The 2014 transparency law of the autonomous community of Catalonia regulated lobbies in the State and the so-called "regulatory footprint".

[19] As Canals points out, the use of Web 2.0 tools will mean a transition from Web 1.0 (public administrations' online presence for the simple dissemination of documents and public information) to Web 2.0 or the collaborative web, where a many people can interact and actively participate by sharing information on digital platforms and social networks,, and where the presence of public administrations implies a greater openness to communication and a more dynamic relationship: D. Canals Ametller. *Transparencia y nuevos cauces de participación de la sociedad civil en el proceso normativo*, in *Revista Informaciòn Comercial Española*, n. 907, 2019, 96.

[20] In fact, within the scope of the General State Administration, the electronic channels were set out in Order PRE/1590/2016, of October 3. This contains the agreement of the Spanish Council of Ministers of September 20, 2016, in which instructions were issued to enable this type of public participation in the regulatory process. The instructions include a definition of ministerial access points as virtual venues that provide two options, "prior public consultation" and "public hearing and information", together with the opportunity for citizens to submit their contributions in a free text box, and also attach documents. Citizens will receive notification of the receipt of their contributions. In order to facilitate participation, the access point will have a search engine to find regulatory projects submitted for consultation, hearing or public information, including those that are still open and those for which the procedure has been finalised. The search engine will use the following search criteria: normative rank, material scope, the wording of the title, open/closed procedure and the deadline date for contributions. It will also include a link to the Transparency Portal. The General Access Point (administración.gob.es) has a link to the participatory access point, and, on its home page, will have a link to the ministerial departments' access points.

and applications in different sectors are obvious, but there are also some disadvantages, especially in terms of ethical implications, respect for people's fundamental rights and, in particular, the right to data protection and privacy. As a result, the law faces major challenges in this area, as regulation is still undeveloped.

In this section we will examine the benefits and drawbacks of using artificial intelligence not only in public administration but also in the management of the regulatory process, and, in particular, how it would help to improve the quality of our regulations. The use of data by public administrations through algorithms would facilitate public decision-making and help assess the effectiveness and efficiency of regulations. This would mean introducing intelligent governance into the regulatory process. Therefore, we will focus on the measures that have been taken both in Spain and the EU regarding artificial intelligence in the field of public administration and then examine its potential use in the regulatory process.

3.1. *Public actions on artificial intelligence*

In recent years, the EU has launched several initiatives in the field of artificial intelligence. For instance, in 2018 the Commission adopted the European AI Strategy which aims to take advantage of the opportunities offered by artificial intelligence and address the challenges it brings.[21] It put people at the centre of the development of artificial intelligence (human-centred AI) and encouraged the use of this powerful technology to help solve some of the world's biggest challenges, from treating chronic diseases, fighting climate change and anticipating natural disasters, to making transport safer, fighting crime and improving cybersecurity.

The White Paper on Artificial Intelligence was also adopted in 2020. It aims to lay the foundations for Europe to combine its technological and industrial potential with a high-quality digital infrastructure and a regulatory framework based on its core values, so that it can become a world leader in innovation in the data economy and its applications, as set out in the European Data Strategy.[22] This will enable the development of an artificial intelligence ecosystem that delivers the benefits of technology to society and the European economy as a whole.

Given the enormous impact that artificial intelligence can have on our society and the need for it to be trustworthy, it is crucial that European artificial intelligence is based on our fundamental values and rights, including those of human dignity and privacy protection. In addition, the use of artificial intelligence systems can play an important role in achieving the SDGs and supporting democratic processes and social rights.

It should also be noted that, in the context of the European Data Strategy, improving access to and management of data is crucial, as it is impossible to develop artificial intelligence and other digital applications without data. The vast amount of new data that will be generated is an opportunity for Europe to become a leader in data and artificial intelligence transformation. Promoting responsible data-management practices and encouraging data compliance with the FAIR principles[23] will help to build trust and enable the re-use of data. Equally important is investment in key IT infrastructure and technologies.

However, as with any new technology, the use of artificial intelligence presents both opportunities and risks. Citizens are concerned that they will be powerless to protect their rights and safety from informational imbalances in algorithmic decision-making, whereas businesses are concerned about legal uncertainty. While artificial intelligence can help protect citizens' security and enable them to enjoy their fundamental rights, there are also concerns that artificial intelligence could have unforeseen consequences or be used for malicious purposes. These concerns must be addressed. Moreover, in addition to the lack of investment and skills, a lack of trust is one of the main obstacles to achieving a wider uptake of artificial intelligence.

It is essential, therefore, to establish a basic regulation in this area that sets out

[21] Published in April, *Artificial Intelligence for Europe* [COM(2018) 237 final.

[22] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Data Strategy*, COM(2020) 66 final.

[23] Namely, easy to find, accessible, interoperable and reusable', as called for in the 2018 Commission FAIR Data Expert Group Final Report and Action Plan (https://ec.europa.eu/info/sites /info/files/turning_fair_ into_reality_1.pdf).

fundamental principles and lays the foundations for the correct use of AI. In this regard, we can highlight the proposal for a European Regulation laying down organizational rules on artificial intelligence presented by the European Commission in April 2021, and pending approval by the European Parliament and the European Council. This regulatory proposal consists of 69 articles divided into 12 titles, together with eight annexes. Its purpose is to regulate artificial-intelligence systems with a view to enhancing their potential benefits and neutralizing their dangers in a way that is compatible with the EU's values and principles. It lays down certain preventive control measures for artificial-intelligence systems and promotes their safe and ethical use by providing a set of rules aimed at mitigating certain risks and negative consequences. To this end, it regulates high-risk artificial intelligence systems and establishes harmonized transparency rules for those systems designed to interact with natural persons for the purpose of generating or manipulating images, audio or video content.

In terms of subjective scope, the proposed European regulation covers all participants in the artificial-intelligence value chain (i.e. providers, importers, distributors) and applies to those located in the EU, as well as those located in a third country if the output produced by the artificial-intelligence system is used in the EU. Regarding objective scope, the proposed regulation classifies artificial intelligence into four risk levels, and imposes more or less stringent obligations depending on their classification:

A) Prohibited systems. This category contains an exclusive list of artificial-intelligence systems that are subject to periodic review and whose use is considered unacceptable due to the risk they pose to safety, life and fundamental rights. The list includes systems capable of distorting human behaviour, making predictions about groups in order to identify their vulnerabilities or special circumstances, or those allowing biometric identification and real-time video mass surveillance by authorities in public spaces. The latter are subject to prior authorization by a judicial or administrative authority, although in justified cases of urgency such authorization may be requested after they have been used. This gives rise to debate as a posteriori authorization may violate data-protection regulations and the fundamental right to privacy.

B) High-risk systems. This category includes other artificial-intelligence systems, which, although not prohibited, pose a high risk to individuals' rights and freedoms and that should therefore be subject to more stringent obligations to ensure their legal, ethical, robust and safe use. This exclusive list is also subject to future periodic review in order to adapt it to new technologies. The systems in this category include safety components for regulated sectors or critical infrastructure such as air transport, motor vehicle surveillance and rail transport. The list also includes systems used for biometric identification and categorization, recruitment, border control, law enforcement and assessing individuals' credit scoring.

C) Medium- and low-risk systems. Systems that do not pose a high risk to rights and freedoms. They include certain less sophisticated or intrusive technologies such as virtual assistants and chatbots.

D) Remaining systems. In principle, these would not be subject to any particular obligation. Moreover, agents in the chain would be free to choose whether or not they wish to adhere to the voluntary compliance systems. Consequently, these systems would in principle fall outside the scope of the regulation.

The proposal also lays down rules on penalties, including fines, applicable to infringements of the regulation. The fines can vary between the following amounts:

A) non-compliance with prohibited practices and data governance obligations by high-risk AI systems: up to €30 million or, if the offender is a company, up to 6% of its total worldwide annual turnover for the previous financial year;

B) non-compliance with any other requirements or obligations: up to €20 million or, if the offender is a company, up to 4% of its total worldwide annual turnover for the previous financial year;

C) supplying incorrect, incomplete or misleading information to notified bodies and/or national competent authorities: up to €10 million or, if the offender is a company, up to 2% of its total worldwide annual turnover for the previous financial year.

In short, as Professor Huergo Lora has pointed out, the European Commission has adopted a regulatory model for artificial

intelligence that includes different administrative-intervention techniques. It combines the total or partial prohibition of certain activities in order to avoid risks (in line with the precautionary principle), with a system of authorisation (preventive control), and ex post control (using this risk-creating technique to impose civil and, where appropriate, criminal liability on those who cause harm). All this, together with an inspection system, usually initiated at the request of the injured parties, which helps the parties and the courts to detect and prove wrongdoing.[24]

We will have to wait until the proposed regulation is finally adopted to see the finished text. Once adopted, the regulation will be directly applicable in all EU countries, which will allow for a harmonized regulation of artificial-intelligence systems throughout the Union.

In Spain, the R&D&I Strategy on Artificial Intelligence was adopted in 2019 and is a key element in the development of the "Coordinated Plan on Artificial Intelligence", adopted by the European Commission at the end of 2018. Furthermore, the Strategy is framed within the Sustainable Development Goals (SDGs), which are set out in the Spanish Action Plan for the Implementation of the 2030 Agenda. It sets out six priorities whose main objective is to make the instruments for promoting R&D&I more effective and to identify how and where technology can help our country grow. It also includes seven recommendations for public policies to align regulatory, structural and organizational adaptations to advances in artificial intelligence. The Strategy is the seed of the Spanish National Strategy for Artificial Intelligence (hereinafter, NSAI) adopted in December 2020, which coordinates state investments and policies to encourage the use of these technologies in our society and economy. It constitutes a reference framework and an incentive for the public and private sectors. In fact, the promotion of artificial intelligence is one of the main elements of the Digital Spain Agenda 2025.[25] This is a key cross-cutting element for transforming the production model and boosting Spain's economic growth in the coming years. As such, the aim is not only to promote research and business innovation in artificial intelligence, but also to use it to transform the economy and society. This includes the functioning of public services, the transparency of public administrations, and addressing major social challenges such as the gender gap, the digital divide and the transition to a green economy. The Digital Spain Agenda 2025 has been updated by the Digital Spain Agenda 2026, which provides a roadmap for the country's digital transformation. This ambitious strategy aims to harness the full benefits of new technologies to deliver stronger and more sustainable economic growth, more quality jobs and higher productivity, contributing to social and territorial cohesion and bringing prosperity and well-being to all citizens.

It is also worth highlighting the economic boost provided by the NextGenerationEU funds. These are available to fund projects aimed at: the digital transition; building technological capabilities; capacity building in strategic digital value chains; accelerating the deployment of infrastructures and very high-capacity networks (especially fibre and 5G) and improving the EU's ability to protect itself against cyber threats; providing safe communication environments, especially through quantum encryption; and ensuring access to data for judicial and political purposes.

3.2. *Artificial Intelligence as a Tool for Better Law-Making*

3.2.1. *The Challenges of Artificial Intelligence in Public Administration*

Artificial intelligence in public administration is still at an early stage of development. However, there are already some very interesting cases,[26] particularly in

[24] *El proyecto de Reglamento sobre la Inteligencia Artificial*, published in the blog *El Almacén de Derecho*, on April 17, 2021 (https://almacendederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial).

[25] Submitted in July 2020, its ninth line of action addresses the data economy and artificial intelligence. The Digital Spain Agenda 2025 can be found at: *https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/230720-EspañaDigital_2025.pdf*.

[26] Cerrillo I Martinez highlights data analysis to predict fire risk to buildings (Atlanta) or flood risk (Hampton), or to identify premises requiring inspection (Las Vegas, Chicago), and even to detect irregularities, fraud and corruption. Natural language processing and machine learning algorithms are also being used to process citizens' requests (Federal Business Opportunities portal). Public administrations use artificial intelligence to support their decision-making process (predictive policing systems, decision support systems for doctors or early

the provision of public services such as transport, security, health, social services and education. Moreover, artificial intelligence is also being used for traffic management and to personalize public services by analysing citizens' personal data and the behaviour of other users through profiling.

However, the main difficulty in integrating artificial intelligence into the activities of public administrations is how to provide legal certainty for the applications and uses of artificial intelligence in public administrations. Without going into the legal nature of the technology itself, or the interesting debate as to whether an algorithm would be a legal regulation and therefore a source of law,[27] different ways have been suggested to provide legal certainty for the use of artificial intelligence in public administration through its regulation. These range from self-regulation by the designers of the IT processes themselves, adopting a completely new regulatory framework; adapting existing regulations, or applying current regulations to emerging artificial intelligence applications.

Given the current development of artificial intelligence in our country, we understand that applying existing legislation could present problems since it is not adapted to new technologies. However, by adapting its provisions to the new situation, we believe that the principles governing the actions of public administrations would be fully applicable and would ensure that the use of artificial intelligence complies with the legal system and fully respects fundamental rights.

To this end, several issues need highlighting. First, we must identify the function that each application or use of artificial intelligence – algorithm – fulfils within administrative actions. In this regard, we can distinguish between predictive algorithms and non-predictive algorithms.[28] As Professor Huergo Lora explains, there are algorithms that can interpret a legal regime to facilitate the administration's decision-making, for instance, programmes that help pay a tax, calculate the grant due to a company under a certain aid scheme, a retirement pension or a teacher's teaching load. They facilitate administrative actions (saving man-hours and minimizing errors) without influencing its content. The programmes are tantamount to a formula that interprets the regulation or rules the administration has to apply (in fact, some legal regulations, bases for tenders or selection procedures already describe the facts using a mathematical formula). Most importantly, it must be possible (in order to check what the administration has done) to apply the regulation 'manually', without the algorithm, to see whether the application of the algorithm is correct or not. The algorithm, therefore, does not affect the content of the administrative action. If the algorithm is incorrect, due to an error in its configuration or application, the result would be unlawful and relatively easy to detect.

There are also algorithms that can be used to mechanise or automate regulated processes – without changing their regulatory framework – but where the process is too complex to be replicated without the algorithm. Therefore, when it is time to monitor the administrative action, it cannot be done without the algorithm and a verification

warning system to prevent school dropouts), or to allocate grants or evaluate teachers (New York). Another AI application is the use of automated response systems to answer questions asked in natural language, or spoken dialogue systems based on voice recognition to provide information, advice and citizen services. So, through chatbots, for example, public administrations can respond to citizens' questions. A. Cerrillo I Martinez, *El impacto de la inteligencia artificial en el Derecho Administrativo, ¿nuevos conceptos para nuevas realidades técnicas?*, in *Revista General de Derecho Administrativo,* n. 50, 2019, 3.

[27] This debate focuses on several issues: 1) not all algorithms used by the public administration produce legal effects; 2) algorithms do not expire once they are complied with or used, and some of them, such as those that use automatic learning, may even lead to innovation in the legal system by incorporating criteria that are not explicitly provided for in the regulation; 3) the procedure for creating algorithms is a long way off from complying with the procedural steps for drawing up regulations and their publication. On this issue, see A. Huergo Lora, *Una aproximación a los algoritmos desde el Derecho administrativo*, in A. Huergo Lora, G.M. Diaz Gonzalez (eds.)*, La regulación de los algoritmos,* Pamplona, Aranzadi, 2020, 64, in which argues that algorithms do not have a regulatory nature. In contrast, A. Boix Palop, *Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisions*, in *Revista de Derecho Público: Teoría y Método*, vol. 1, 2020, argues that the algorithms used by public administrations for the effective adoption of decisions must be considered regulations because they fulfil a material function which, in a strict sense, is equivalent to that of legal rules, as they regulate and predetermine the actions of the public authorities.

[28] A. Huergo Lora, *Una aproximación a los algoritmos desde el Derecho administrativo*, 68.

of how it has worked is needed. This is the case with complex processes to allocate limited resources (e.g., competitive internal promotions for a large number of civil servants, as was the case in Italy, or the allocation of internal-medicine residency positions, which was suspended as a precautionary measure by the Admnistrative Chamber of the Spanish Supreme Court in 2020), where the individual results are interrelated. The legal control of such algorithmic decision-making cannot simply be a matter of manually applying the rule to see if it is consistent with algorithmic performance. Instead, the functioning of the algorithm must be examined, which requires knowledge of all the factors involved in determining its result.

Other algorithms help to steer administrative action in a certain direction and, unlike those mentioned above, provide their own decision-making elements. These are predictive algorithms and represent artificial intelligence in the strict sense of the word. Normally, their effect is equivalent to a scale, which is one of the most common ways of managing administrative action. In this case, however, the scale is not set by a regulation or a non-regulatory administrative decision (such as a set of specific administrative clauses or the terms and conditions of a tender), but by the algorithm itself, based on an analysis of previous cases. The algorithm is designed to achieve an objective set by the regulation, such as identifying students who are at risk of educational underachievement. It does this by creating a 'portrait' based on an analysis of data collected in previous years. The specific characteristics of the portrait are not determined by a person, but by the algorithmic model. Such models are currently used (without regulatory authorization) to support decisions to initiate proceedings, or, at a lower level of legal finalization, to channel the use of public welfare or surveillance resources (e.g. to identify individuals who may require tracing due to an undetected risk situation). In the absence of an algorithm, such decisions would, in practice, lack legal control (they are not discretionary administrative acts, but informal or procedural measures), so the risks involved in the use of these algorithmic models is limited.

To ensure that public decisions do not discriminate against individuals or groups, it is important to avoid bias in both data and algorithms. Discrimination may indeed occur as a result of the data used. If data are of poor quality, contain errors, are flawed, or reflect pre-existing patterns of inequality and discrimination that are consciously or unconsciously transferred to the algorithm, it will learn from biased data or data that discriminate based on gender, race or other conditions, and will make bad decisions or decisions that lead to discrimination. Moreover, the biases may be in the algorithms themselves, and may have been introduced intentionally or unintentionally by the designers or users of the algorithms. In either case, bias can lead to discriminatory decisions by public administrations. To avoid this, data quality must be improved and algorithms should be designed to be particularly sensitive to possible discriminations. In addition, there is a need to encourage the participation of stakeholders in algorithmic decision-making and more broadly, the participation of citizens in the design of algorithms.[29]

It is noteworthy that scholars have called for the creation of committees of experts or other interdisciplinary collegiate bodies which also include representatives of society, to monitor the development of algorithms and, more generally, to assess the impact of artificial intelligence on society and carry out risk analyses.[30] It is also important to create a register of artificial intelligence algorithms and systems used by public administrations. This should be accompanied by a system for certifying that the systems comply with the prevailing regulations and codes. Periodic inspections or audits to check the functioning of the algorithms should also be carried out.[31]

[29] A. Cerillo I Martinez, *El impacto de la inteligencia artificial en el Derecho Administrativo, ¿nuevos conceptos para nuevas realidades técnicas?*, 16.

[30] See in this regard D. Canals Ametller, *Incidencia del avance tecnológico en el derecho público (elaboración, práctica, docencia e investigación)*, in B. Puentes Cociña (ed.), *El derecho ante la transformación digital: oportunidades, riesgos y garantías*, Barcelona, Atelier, 2019, 31-50.

[31] In O. Cortes, *Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración pública*, in *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 18, 2020, 59, the author states that the register would be used, if necessary, to interrupt the use of those algorithms that do not adequately fulfil their function or that show behaviour at variance with what is expected. Regarding periodic inspections, these would be used to ascertain how the registered algorithms are performing. This would involve an audit or inspection of their performance, both in terms of regula-

Another important issue is the need to guarantee the transparency principle in the use of artificial intelligence in public administrations.[32] This requires addressing the opacity that characterizes algorithms, an opacity that has led to them being called 'black-box algorithms'. Algorithmic opacity may be due to a lack of access to information, or because accessible information on algorithms does not actually exist. The technical complexity of algorithms makes them difficult for citizens to understand, and therefore renders them inaccessible. Whatever the case, the fact is that public administrations do not formalize their decisions to use algorithms, nor do they document the sources or the results obtained by the algorithms. In our view, administrations should provide access to the content of the algorithms. Moreover, they should formalize and document the decision to use artificial intelligence, including details of its purposes, resources, results, etc., and most importantly, provide an explanation of how the algorithms work and a rationale for the results obtained. These actions, combined with audits of how the algorithms actually work, would guarantee transparency. Despite the complexity of artificial intelligence, under the transparency principle, it should always be possible to justify any decision taken with the help of artificial intelligence that may have a significant impact on people. Furthermore, it should always be possible to simplify the calculations of the artificial-intelligence system in order to make them understandable,[33] because algorithmic transparency is the only way to build a healthy digital public administration.[34]

The need to achieve interoperability between different public administrations has also been called for, since artificial intelligence does not recognize national and regional governments or borders. At present, the difficulty lies in the fact that each public authority has established its own trust framework, which prevents cross-border exchanges and hampers the functioning of the single market for businesses and citizens.[35] With this in mind, the EU adopted Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. The regulation addresses the need for administrative cooperation based on a review of the European Interoperability Framework, and aims to improve digital cooperation between public administrations in Europe through the free flow of data.

Finally, it is essential that the use of artificial intelligence in public-administration activities respects data protection and privacy rights, and is compatible with the protection afforded to these rights by the legal system at both the European and national levels. As such, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Spanish Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights, ensure a high level of protection of personal data and incorporate data-protection principles at the design phase and by default.

tory compliance and ensuring that they are performing according to the law. Control could be exercised over the results provided by the systems - ex ante, before the results become effective, or ex post once effectiveness has been achieved – and even over the training of the algorithms, by supervising the information provided for their learning and checking their effects before they are put into operation.

32 In this regard, A. Merchàn Murillo, *Inteligencia artificial y blockchain: retos jurídicos en paralelo*, in *Revista Española de Derecho Administrativo*, 50, 2019, 25, points out that the use of artificial intelligence by public administrations will require reconciling the transparency principle and publication of administrative documents with personal-data protection and the privacy rights under a clear and explicit regulatory framework.

33 A. Merchàn Murillo, *Inteligencia artificial y blockchain: retos jurídicos en paralelo*, 12.

34 G. Vestri, *La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa*, in *Revista Aragonesa de Administración Pública*, 56, 2021, 382. The author argues that algorithmic transparency should be approached from two angles. On the one hand, there is a clear need to ensure that the public administration's choice of algorithm is transparent. On the other hand, it must be possible to verify the transparency of the algorithm when it is in operation in the public administration, thus guaranteeing that an interested party can determine how algorithms make decisions. In this way, a double level of transparency can be achieved, which is vital given the intangibility of an algorithm. A distinction is thus made between ex ante transparency (during the contracting or provision phase of the artificial intelligence system) and ex post transparency (once the artificial intelligence system is up and running).

35 In this regard, see A. Merchàn Murillo, *Inteligencia artificial y blockchain: retos jurídicos en paralelo*, 10.

In short, the process of adapting our administrative legal system to take advantage of the benefits and opportunities offered by artificial intelligence and improve administrative action involves determining how to control algorithms so that they do not violate citizens' rights.[36] These controls should be exercised at different levels.[37] Thus, at the European level, a European artificial-intelligence agency could be set up to define European policy and strategy in this area and monitor algorithms in general. Indeed, the regulatory-framework proposal on artificial intelligence proposes the creation of a European Artificial Intelligence Board comprising high-level representatives of the competent national supervisory authorities, the European Data Protection Supervisor and the Commission. Its role, however, will be to facilitate the smooth, effective and harmonized implementation of the new regulation, rather than to monitor or supervise. The Board will issue recommendations and opinions to the Commission on high-risk artificial intelligence systems and on issues related to the effective and uniform application of the new regulation. It will also act as a centre of expertise for national authorities, contributing to the development of specialist knowledge and supporting standardization activities in this area.

At the national level, the monitoring and supervisory functions could be entrusted to the Spanish State Secretariat for Digitalisation and Artificial Intelligence[38] or to a newly created body under the Secretariat.

A final level of control would be exercised by the courts. The administrative control they exercise would become an intelligent automated administrative action, whose limits and adaptation to the legal system of the algorithmic administration would be determined by a judge.

3.2.2. *Artificial Intelligence in the Regulatory Process*

As mentioned above, we are convinced that artificial intelligence can contribute to making better regulations. Since there are no specific rules for its use in regulatory proceedings, it is necessary to apply the criteria set out in Spanish Law 40/2015, on the Legal Regime of the Public Sector (hereinafter, LRJSP) for electronic administrative actions in the processing of administrative procedures.

First, we would like to point out that although artificial intelligence can clearly facilitate the exercise of regulated powers,[39] its use in the exercise of discretionary powers is less clear. In such cases, the Administration determines the rights, goods or interests that should remain outside the scope of artificial intelligence, so that they cannot be replaced by an algorithm, even if it is technologically possible to do so. In other words, certain decisions should be left to human discretion, a concept that has been referred to as the "reserve of humanity"[40]. It is true, however, that the greatest efficiency gains are to be found in discretionary decision-making using artificial-intelligence tools. Here, the transformation is qualitatively different in those areas where increased computational capacity allows for new inferences and a better identification of situations, causes or possible solutions. In this case, the increase in efficiency is linked to an improvement in the ability to use these tools to evaluate situations or take decisions that are different from those that would have been taken or are generally taken by human beings, and that are also not

[36] See C. Campos, *Inteligencia artificial e innovación en la Administración pública: (in)necesarias regulaciones para la garantía del servicio público*, in *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 3, 2019, 74-91.

[37] In this regard, see O. Cortes, *Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración pública*, 54-63.

[38] Set up pursuant to Royal Decree 403/2020, of 25 February, which develops the basic organisational structure of the Ministry of Economic Affairs and Digital Transformation. Under the head of the Ministry, this body will, within the scope of its competences, exercise the functions set out in art. 62 of the LRJSP, regarding the promotion of the digitalisation of society and the economy in a way that respects individual and collective rights, as well as the values of the legal system (art. 8.1).

[39] As is well known, and as García de Enterría and Tomás Ramón Fernández point out, it is assumed that "the Law can exhaustively determine each and every one of the conditions for the exercise of the power, in such a way as to construct a complete legal provision and a power applicable to it, which is also defined in all its terms and consequences (for example, retirement based on a civil servant's age, promotion based on length of service, tax settlement - application of a quota established by the Law to a base established on a specific taxable event - etc.)". In these cases, "the Administration functions in a way that could be called automatic.", *Curso de Derecho Administrativo,* vol. I, 11th ed., 2000, 454

[40] J. Ponce Solé, *Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico*, in *Revista General de Derecho Administrativo*, 50, 2019, 28.

easily anticipated or foreseen by normative and regulatory instruments. And it is in these cases that the greatest risks lie, because the functioning of this type of programme is unknown, in other words, there is a black-box effect. This can prevent programmers from reliably predetermining the specific results of the programme once it has been executed, forcing them to rely, to a certain extent blindly, on the validity of these results based solely on the assumption that the programming has been carried out correctly. It is here that public law must take a stand and provide a legal response.[41]

So far, German public law has expressly prohibited, in its administrative procedure act, the use of algorithms for the adoption of decisions affecting citizens' rights that may have a discretionary content, whereas art. 41 of our LRJSP only regulates simple automated decisions.[42] However, this is an issue that should be reviewed sooner rather than later, as it seems that applying the precautionary principle to automated administrative actions in such a strict way may conflict with the principle of effectiveness.

In any case, and without knowing what the future of administrative law will be in this matter, as far as legislative and regulatory power is concerned, it is a discretionary power, but with regulated procedures. The discretionary nature of this power has added value for discretionary administrative acts, as it involves the decision to regulate an issue by creating a legal regulation that will eventually become part of the legal system, with all that this entails. We believe that the will to decide to regulate a matter, as well as the motives and reasons for doing so, i.e. the adoption of the initiative itself, cannot be left in the hands of artificial intelligence (it is difficult to imagine that a computer programme could ever demonstrate this will), but there are some procedures within the complex regulatory process that could be speeded up by automated administrative action and artificial intelligence tools, thus leading to better regulatory quality.

We should remember that art. 41.1 of the LRJSP states that an automated administrative action is "any act or action carried out entirely by electronic means by a public administration within the framework of an administrative procedure, and without the direct intervention of a public employee." In this type of action, the competent body or bodies responsible for defining the specifications, programming, maintenance, supervision and quality control and, where appropriate, auditing of the information system and its source code, must be designated beforehand. The body responsible for reviewing challenges must also be identified. This will ensure that competence is exercised only by the body assigned such competence, i.e. it must have the effective capacity to monitor the functioning of the algorithms.

In any case, given that the exercise of regulatory power is clearly the responsibility of the body to which it has been delegated, and that this body is responsible for supervising the algorithms used in the regulatory process, the prior consultation, hearing and public-information procedures can all be fully automated. These procedures channel public participation in the regulatory process and, as we have seen, so far only electronic means have been regulated, but we must be aware of the power of social networks and platforms to channel information. Therefore, we are mindful of the fact that public participation in the regulatory process through social networks would allow us to obtain valuable information that, processed with artificial intelligence, would help public bodies make regulatory decisions.[43] Admittedly, the use of social networks as a channel for digital participation still poses challenges, as, given the existing digital divide, it creates inequalities. Moreover, the use of social networks by public administrations is still very limited and those that do use them (mainly local authorities) do so in the same way as other regular users of the network.

Similarly, we have the example of the US, where federal agencies are embracing technological innovation in the regulatory process by using computerized text analysis

[41] A. Boix Palop, *Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisions*, 230.

[42] I. Martín Delgado, *Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada*, in *Revista de Administración Pública*, 180, 2009, 371, also suggests prohibiting administrative decisions with a significant discretionary content.

[43] See in this regard, D. Canals Ametller, *El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos)*, 11.

(eRulemaking) for citizen participation. This is carried out on a digital platform that encourages high participation and whose results are evaluated using artificial intelligence. Thus, in the phase prior to the drafting of regulatory standards, the pre-regulatory process (notice-and-comment) is managed electronically and new technologies are used to distribute information and collect comments from the public on regulatory initiatives via a single online platform.[44]

This model has been the subject of several studies which show that incorporating new technologies into the regulation-making process serves four purposes: first, transparency and participation in the content of the regulation increases its democratic legitimacy; second, regulatory quality is improved because eRulemaking provides additional information, including information on the impacts of a specific rule or regulation and the positive and negative effects of the measures or other regulatory options; third, greater efficiency is achieved since it reduces the operating costs of the federal agency concerned; and fourth, there is increased compliance with regulations by addressees and public administrations as greater regulatory transparency implies greater acceptance and facilitates judicial control.[45]

However, a shortcoming of the American model is the fact that increased public participation does not always translate into quality information. Thus, one of the current challenges of eRulemaking is to ensure that new technologies effectively improve the quality of citizen participation and regulations. Nevertheless, it is clear that interest in the regulatory process has increased significantly in the United States. There has also been a considerable increase in public participation, with US agencies receiving millions of comments each year from citizens and organisations representing a wide range of interests regarding their respective regulatory proposals. These comments are a valuable source of information that can be used to examine empirically how public agencies relate to citizens. Indeed, several such analyses have already been undertaken.[46]

Furthermore, this information and the vast amount of data it generates can also be used to improve the public decision-making process. Thus, we can distinguish between different types of regulatory data: (a) data prior to the adoption of a regulatory initiative (empirical and/or specialized data and information used to make regulatory decisions. These data are obtained from the results of prior consultations, hearings and public information procedures, sectoral institutional reports, monitoring and supervisory bodies, analyses of case-law outcomes, academic research, and participation on platforms and social networks, as discussed in this paper); b) data following the adoption and entry into force of the regulatory provision, and in particular, data on the effective implementation and enforcement of legal regulations; and c) official data from the legal systems in force, given the large number of regulations and regulatory types, the lack of clarity of which urgently calls for simplification and streamlining of legal sources.[47]

The benefits of using digital technologies in the regulatory process are obvious. They can assess citizen participation, interpret the impact of regulation or its degree of

[44] For L. Arroyo Jiménez, *Participación electrónica y elaboración de normas administrativas en España y en los Estados Unidos de América*, in I. Martin Delgado (ed.), *La reforma de la administración electrónica: una oportunidad para la innovación desde el derecho*, Madrid, INAP, 2017, 231-258, eRulemaking is a different approach to processing and resolving regulatory procedures; it is a way of managing procedures to make regulations based on the use of new information and communication technologies that go beyond mere websites. This is because tools such as those enabling electronic claims or public meetings can be incorporated into the procedure, and social networks, blogs or other applications can increase transparency and citizen participation.

[45] D. Canals Ametller, quoting Professor Arroyo, in *El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos),* 13.

[46] See M.A. Livermore, V. Eidelman, B. Grom, *Computationally Assisted Regulatory Participation*, in *Notre Dam Law Review,* vol. 93, issue 3, 2018, 977. These authors have conducted a large-scale "sentimental analysis" of public comments, to see how word choices in millions of public comments relate to measures or ideology in a variety of settings and to assess what attitudes are reflected in the texts. Having applied a basic and replicable sentimental analysis procedure to public comments received for all non-minor regulations over the course of the Obama Administration, they found that administrative agencies with more moderate ideological leanings tend to receive comments containing more positive language. Such analysis indicates that the agencies' political characteristics are correlated with the characteristics of the comments. As noted by D. Canals Ametller, *El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos)*, 16.

[47] As argued by D. Canals Ametller, *El proceso normativo ante el avance tecnológico y la transformación digital (inteligencia artificial, redes sociales y datos masivos),* 17.

compliance; facilitate regulatory assessment (both ex ante and ex post), provide greater regulatory transparency and produce information on how to regulate certain situations. Having access to this privileged information undoubtedly leads to improved regulatory quality. We therefore believe that implementing artificial intelligence tools would significantly speed up these processes and help Spain rank among the most advanced countries in terms of regulatory improvement.[48]

Although administrative law will eventually have to address this issue, we would like to think that progress is being made in this area. In this regard, we can highlight the adoption of the Digital Rights Charter, one of the commitments made by Spain in the Digital Spain 2025 plan, which recognizes the challenges posed by the adaptation of current rights to the virtual environment. It includes a set of principles and rights to guide future regulatory projects, and public policies to guarantee the protection of individual and collective rights in the new digital environment.

The Charter is a non-binding soft law document that recognizes and demands the protection of rights already provided for in Spanish Organic Law 3/2018, of 5 December, on Data Protection and the Guarantee of Digital Rights. It includes new contributions regarding the protection of the elderly and people with disabilities in the digital environment, conditions for health protection in the digital environment, and, above all, and of particular interest to us, rights regarding artificial intelligence (section XXIII of the Charter). More specifically, it includes the right to algorithmic non-discrimination; it ensures transparency, auditability, explainability and traceability, and it guarantees accessibility, usability and reliability. The will of the individual prevails, in such a way that individuals "have the right not to be subject to a decision based solely on automated decision-making processes, including those using artificial intelligence procedures, that produce legal effects or significantly affect them in a similar way (…). In such cases, the following rights are recognized: a) the right to request human supervision and intervention, b) the right to challenge automated or algorithmic decisions." As such, individuals "shall be informed of the use of AI systems that communicate with human beings using natural language in all its forms. In all cases, assistance from a human being at the request of the interested party shall be guaranteed. The use of AI systems aimed at psychologically manipulating or disturbing persons, in any aspect affecting fundamental rights, is prohibited."

Indeed, the Charter is a programme-outcome document that provides a roadmap for addressing the challenges of adapting existing rights to the virtual environment. It does not create new rights, but rather protects existing rights in the context of digital competencies. Although its lack of regulatory value prevents the rights recognised in the Charter from being binding, this is not its purpose. Instead, it is intended to reflect the existing trends and realities of contemporary society, and serve as a guide for future regulatory adaptation and development. The introduction to the Charter clearly states that its objectives are threefold: to describe the impact and consequences of digital

[48] As is well-known, to measure regulatory improvement at the international level, a series of indicators - Indicators of Regulatory Policy and Governance (iREG) - were drawn up by the OECD in 2015 to measure countries' regulatory quality. The 2018 OECD Regulatory Policy Outlook report - which analyses countries' initiatives to improve regulatory quality when compared to the principles set out in the 2012 OECD Council Recommendation on Regulatory Policy and Governance - notes that Spain is gradually expanding its better regulation agenda, which initially focused on simplifying administrative burdens, stakeholder participation and evaluation. Thus, an easy-to-navigate platform was created, the "Transparency Portal", where the Annual Regulatory Plan can be consulted and which allows for public consultation, although stakeholder participation has not yet been systematically carried out.
Along the same lines, the regulatory impact analysis report must, and in practice does, accompany all regulatory projects. The updated 2009 Methodological Guide will provide regulators with an effective tool for improving the preparation of the regulatory impact-analysis report. It has been suggested that the guide could go further by providing advice on data-collection methods and clear and transparent methodologies for assessments. The report also notes that Spain would benefit from developing standard techniques for ex post evaluation, which is still in its infancy and not yet systematically implemented. It mentions the Office of Regulatory Coordination and Quality as a regulatory oversight body that was launched in 2018 to oversee the implementation of regulatory improvement requirements, specifically by examining the contents of regulatory impact-analysis reports and ex post assessments. However, despite these improvements, Spain is below the OECD average in key areas (public participation, ex ante assessment, regulatory impact analysis reports and ex post assessment).

environments and spaces; to anticipate future scenarios that can be predicted; and to revalidate and legitimize the principles, techniques and policies that, based on the culture of fundamental rights, should be applied in current and future digital environments and spaces.

Therefore, we see the Charter as a step forward in the digital transformation of public administration and in line with other initiatives that have been carried out in this area. Such initiatives include the proposed European Regulation on artificial intelligence, and the Portuguese Charter of Human Rights in the Digital Age (Law number 27/2021, of 17 May). Portugal has followed in the footsteps of other countries that have adopted specific laws to recognize rights in the digital environment, for instance, the French Digital Republic Law of 2016, while Spain has aligned itself with Italy, which adopted its Declaration of Internet Rights in 2015.

The Spanish National Plan for Digital Skills, included in the Digital Agenda 2026 and which part of Spain's Recovery, Transformation and Resilience Plan, is also noteworthy. The Plan's objective is to ensure the digital training and inclusion of all workers and citizens in order to foster the creation of quality jobs, reduce unemployment, increase productivity and, above all, contribute to closing gender, social and territorial gaps.

Irrespective of the model chosen to develop artificial intelligence in public administration, this process must be accompanied by a plan to specialize technical resources and infrastructures, together with the introduction of a package of measures aimed at the training and specialization of public-administration staff.

4. *Criteria for Regulatory Rationality*

The drafting of poor-quality regulations is not only detrimental to legal certainty but also to legal rationality. We therefore believe that the only way to achieve quality rules in our legal system is to develop criteria and key elements that must be considered when drafting rules, together with the introduction of artificial intelligence into the regulatory process. We believe that different types of regulatory rationality should be introduced in Spain that include several criteria.[49] Namely:

A) Linguistic rationality. If a regulation is not clear and understandable, it will be difficult to comply with it. Thus, it must be clear, precise and simple, so that the main addressee of the regulation, the citizen, can understand its content. Moreover, if the regulation concerns technical or complex issues, descriptive elements or definitions must be introduced. But we must go further and appreciate the importance of language, using simple, precise vocabulary and avoiding ambiguity and redundancy. To achieve this, training should be provided for civil servants or experts who draft regulations. We must not forget that our legislators are no longer, as in the past, made up of learned people.[50]

B) Logical rationality. The regulation must be consistent with existing laws and avoid repetition or reiteration of other regulations. Systemic repetition of higher regulations in a higher rank are common. References and cross-references should be used as this avoids unnecessary proliferation of legal regulations.

C) Formal or technical rationality. The procedure established for drafting and approval must be followed and, in order to have legal effect, it must be published in the appropriate Official State Gazette. Within the drafting procedure, it is essential that the regulatory impact-analysis report justifies the necessity and proportionality of the regulation, and that the economic report supports the budgetary availability for its implementation. The *ex ante* assessment should provide all the necessary information on the regulation and allow us to extract its regulatory footprint.

D) Systematic rationality. Regulations must have a logical and systematic order that gives meaning to their content. To this end, the current guidelines establish a basic structure. Regulations must have a title, an

[49] Several years ago, the authors M. Atienza, *Contribución a una Teoría de la Legislación, Cuadernos* Civitas, Santander, Editorial Civitas, 1997, 27 and 28, and A. Calsamiglia, Ciencia Jurídica, *El Derecho y la Justicia*, in *Enciclopedia Iberoamericana de Filosofía*, 11, Madrid, Editorial Trotta, 1996 suggested providing the norms with higher quality standards in the following areas: 1) communicative or linguistic; 2) formal jurisdiction; 3) pragmatic; 4) teleological, and 5) ethical.

[50] As was the case in the age of the Enlightenment, when the legislative assemblies were made up of "learned and eloquent men who confer amongst themselves, who discuss the most sublime matters, who dispute with heated interest or offended self-esteem, and in who do not decide the plurality of votes, but after long examination and great debates...". J. Bentham, *Estilo de las leyes*, in *Tratados de Legislación Civil y Penal*, Madrid, Editora Nacional, 1981, 536.

explanatory part (preamble or explanatory statement), proposals (articles), a final part (transitional, final, derogatory provisions, etc.) and, where appropriate, annexes. In addition, everything must follow a systematic order so that the content of the regulation is logically distributed within its titles or chapters.

E) Teleological rationality. The quality of the regulation should not only address its formal or technical quality, but also its material quality. An ex post evaluation of the regulation should be carried out to ensure that the objectives pursued have been achieved and that the costs and burdens derived from it were justified and adequately assessed.[51] An adopted regulation must be evaluated to see whether it satisfies basic standards of rationality and reaches acceptable levels of clarity, coherence, efficacy, effectiveness, axiological suitability and efficiency, criteria which, if properly applied, make it possible to distinguish between good and bad legislation.

F) Organisational rationality. Another important issue is the need for coordination between the various bodies responsible for regulatory oversight. The OECD itself has pointed out that oversight mechanisms are essential in order to reduce the gap between the formal requirements of better regulation instruments, their practical implementation and the necessary cultural change. Although administrative organisation varies from one country to another, public policy, by virtue of its cross-cutting nature, is subject to fragmented governance, where different bodies are assigned oversight functions in regulatory quality-improvement policy. In Spain, there are several ministries with competences in this area, for example: the Ministry of Territorial Policy and Public Function, which is responsible for fostering the simplification of administrative procedures, monitoring the reduction of administrative burdens, ensuring the transparency of public actions, promoting the Administration's digital agenda and encouraging citizen participation in the regulatory drafting process; the Ministry of Economy and Business, which checks various aspects of the quality of the economic impact analysis: general, sectoral, on market unity, competition and competitiveness, and plays a key role in the ex post evaluation of the results of the regulation; and the Ministry of Industry, Trade and Tourism, which is responsible for assessing the economic impact of regulations on small and medium-sized enterprises (SMEs). In addition, there is the Office of Coordination and Regulatory Quality, which is part of the Ministry of the Presidency, Parliamentary Relations and Equality and is responsible for promoting the coordination and quality of the government's regulatory activity, and the Council of State, which is responsible for assessing the legality of regulations, the processing procedure, the efficiency of the Administration in achieving its objectives, and the legal quality of regulations and draft bills. All these, together with other bodies that also participate in the regulatory cycle, in addition to those that draft and process regulatory projects, such as the General Technical Secretariats of all the various ministries, the National Commission for Markets and Competition or the General Codification Commission. Therefore, this is another issue that we should address and one in which we should strive for organisational simplification, as this is the only way to ensure that supervisory functions can be carried out responsibly, independently and transparently.

G) Technological rationality. Lastly, and in line with what we have analysed in this paper, we should be committed to introducing technological innovation into the regulatory process. There are many benefits to be gained from using artificial intelligence for to assess and interpret of the huge amount of regulatory data generated throughout the process. These range from improving citizen participation by enabling the use of platforms and social networks for prior consultation, providing

[51] Regarding the ex post evaluation of regulations, the questions Atienza suggests we ask ourselves could be useful: First, what are your goals? Are there any undeclared objectives or results (required or not by the "legislator")? Are they justified according to socially dominant values, constitutional principles or certain ethical concepts? Also, in relation to more technical matters: are the contents of the law (the obligations, prohibitions and permits it contains) and the institutions that it considers, appropriate to achieve the objectives? Are there incentives (positive or negative sanctions) and resources (for example, financial) that can ensure the effectiveness of the law? Does the law leave gaps or create contradictions or, on the contrary, does it regulate everything it should regulate and does it do so harmoniously, taking into account all the articles and the rest of the legal system? Finally, is it written in such a way that the regulation's message is reasonably clear and can be understood by its addressees - direct and indirect – and does not give rise to interpretive problems that could have been avoided?: M. Atienza, *Sobre la nueva Ley de Reproducción Humana Asistid*a, *in Revista De Bioética y Derecho*, 2009, vol. 14, 4.

information and public hearings, to strengthening regulatory evaluations (ex ante and ex post) and measuring the degree of acceptance and compliance with the regulation. All this will improve regulatory quality and the regulatory decision-making process.

We believe that the content of the regulation is as important as its effectiveness. In other words, "it is not enough just to examine the regulations in the abstract, we must also see how they actually work."[52] The criteria for regulatory rationality would allow us to guarantee the principle of legitimate expectations, which is key to protecting citizens' rights in the face of unforeseeable regulatory changes. This includes not only the protection of citizens' legitimate expectations, who adapt their economic behaviour to existing legislation in the face of regulatory changes that are not reasonably foreseeable, as established by case law,[53] but also, and more importantly, protecting against unnecessary regulations that disrupt, complicate or make the application of existing legislation more difficult.[54] This is the only way to comply with art. 3.1.e) of the LRJSP which stipulates that public administrations must observe the principles of good faith and legitimate trust in their actions.

The regulatory rationality test should be carried out during the initial phase of each regulatory development process by a specialised body created ad hoc in each public administration with regulatory powers, given that both the legislative initiative and regulatory power are vested in the government (either state or autonomous, or even local in the case of local governments' regulatory power). Thus, when the regulation reaches the parliamentary-debate stage (in the case of laws), its text already meets all the linguistic, technical and formal criteria.

[52] A. Nieto, *El Derecho comunitario europeo como derecho común vulgar*, in *Revista de Administración Pública*, no. 200, 2016, 28.

[53] For clarification, we can highlight the Spanish Supreme Court decision of June 23, 2014, which states that "The principle of the protection of legitimate expectations is neither new nor unusual in our jurisprudence. Several judgments have made it operational in different areas to safeguard those who have acted under its protection. These include the judgments of November 23, 1984 (official case repertory 1984/5956), June 30, 2001 (cassation 8016/95), April 26, 2010 (cassation 1887/05), November 28, 2012 (cassation 5300/09) and January 22, 2013 (cassation 470/11). The last two judgments, passed with regards taxation, adopt the criteria already established in the case law of the European Court of Justice, according to which the principle is binding on all public authorities: (i) if the belief of the administration that supports it is based on external signs and not on mere subjective appraisals or psychological convictions and, (ii) assessing the interests at stake, the situation of those who have legitimately relied on the Administration is worthy of protection [Judgments of April 26, 1988, Krüechen (316/96); 1 April 1993, Lageder and others (joined cases C-31/91 to C-44/91); 5 October 1993, Driessen and others (joined cases C-13/92 to C-16/92); 17 July 1997, Affish (C-183/95); 3 December 1998, Belgocodex (C-381/97); and 11 July 2002, Marks & Spencer (C-62/00)].

[54] Similarly, S. Muñoz Machado, *Regulación y confianza legítima*, in *Revista de Administración Pública*, no. 200, 2016, 160.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 225-231
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 19

*A Few Observations on Some Current Issues in the Digital Revolution of Cultural Heritage**

Maddalena Ippolito
(PhD Student in Legal Sciences at the University of Foggia-Siena)

ABSTRACT The paper, tackling the highly topical issue of the digitalization of cultural heritage, dwells on the articulated reform process aiming at the digitalization of cultural heritage and emphasises the true social function of cultural property, whose universal availability is the ultimate goal pursued by Article 9 of the Constitution. The observations are based on the recent orientations of the Recovery and Resilience Plan, focusing on the analysis of the impact of artificial intelligence in the digital revolution of cultural heritage. In this perspective, the focus is on how the use of emerging technologies can act as a driver of new ways of valorising cultural property which exploit both the attractiveness potential of the property and innovative models of content presentation. The option to implement new technologies to cultural heritage is part of a more general vision focused on the possible "birth" of a digitalized cultural property that draws its cultural "value" from the intangible dimension of the basic asset. The idea behind the reflections that follow aims to overcome the "cosità" of things that are part of digitalized cultural property to dwell on the intangible value of the property to give it greater relevance and protection.

1. *Introduction*

In the never-ending process of digital revolution of public administrations, the use of artificial intelligence is seen as an essential tool to ensure new forms of protection, valorisation and fruition of cultural heritage.

Therefore, a way to achieve this goal is to create a new relationship between technology and cultural heritage. A relationship that is not limited to the preservation of cultural heritage but aims to rethink the collaboration/interaction between public administration and the private sector as a part of horizontal subsidiarity falling within the framework of horizontal subsidiarity pursuant to art. 118 (4) of the Italian Constitution.[1]

And so, in an organic system of digital revolution, the use of strategies based on a virtual use of cultural heritage enables the development of digital services and the development of applications for the creation of a distributed ledger and promotes the creation of new digital-cultural contents to stimulate an economy based on the circulation of knowledge.

The observations that can be drawn from the analysis of this phenomenon lead to a necessary rethinking of existing legislative provisions that reflect the latest technological innovations and the impact of these on current legislation.

Against this background, the true social function of cultural property, i.e. universal fruition, should be carefully emphasised: a social function that can be attributed not only to digitally-born cultural property, but also to digitally-transcended cultural property, as the ultimate objective set out in Article 9 of the Italian Constitution.[2]

* Article submitted to double blind peer review.

[1] On the principle of horizontal subsidiarity, intended as a vehicle for the transformation of the "methods of democracy", see the approach of Council of State, Section consultative for regulatory acts, 25 August 2003, in *Giurisprudenza italiana*, 2004, 716, on which see, for further details, G. Razzano, *Il Consiglio di Stato, il principio di sussidiarietà e le imprese*, in *Giurisprudenza italiana*, n. 4, 2004, 716. For a further study on the principle of horizontal subsidiarity, see, *ex plurimis*, E. Follieri, *Le funzioni amministrative nel nuovo Titolo V della parte seconda della Costituzione*, in *Le Regioni*, 2-3, 2003, 444; G.U. Rescigno, *Principio di sussidiarietà orizzontale e diritti sociali*, in *Diritto pubblico*, 2002, 19; G. Arena, *Il principio di sussidiarietà orizzontale nell'art. 118 u.c., Costituzione*, in *Studi in onore di Giorgio Berti*, Naples, Jovene, 2005, 179; S. Cassese, *L'aquila e le mosche. Principio di sussidiarietà e diritti amministrativi nell'area europea*, in *Foro italiano*, V, 373; V. Cerulli Irelli, *Sussidiarietà (dir. amm.)*, in *Enciclopedia giuridica*, Agg. XII, 2004, 1.

[2] See F. Santoro Passarelli, *I beni della cultura secondo la Costituzione*, in *Studi per il XX anniversario dell'Assemblea Costituente*, II, Florence, Vallecchi, 1968, 436, who says that "in the overall evaluation of the constitutional text, it seems to be clear that the protection of cultural property is a corollary of the fundamental rule concerning the development of culture and this protection must be oriented in the most appropriate direction to achieve the use of property as an instrument of culture". See also F. Merusi, Sub *Art.* 9, in G. Branca (ed.), *Commentario alla Costituzione*, *Art. 1-12 Principi fondamentali*, Bologna-Rome, Zanichelli-Il foro italiano, 1975, 434; A. Sandulli, *La tutela del paesaggio nel-*

And also, in line with the recent guidelines of the Recovery and Resilience Plan,[3] the focus will be on the potential "birth" of a digitalized cultural property that draws its cultural "value"[4] from the intangible dimension of the basic property.

2. *The Universal Fruition of Digital Cultural Heritage*

Undoubtedly, one of the factors leading to the digital reinterpretation of the fruition of cultural heritage is a renewed interpretation of the whole of public activities through which the administration pursues the interest of the community to universally enjoy the multiple cultural values expressed by our historical and artistic heritage.[5] In the digital transition, the preservation and valorization of cultural property[6] is flanked by "the constitutional duty to promote culture (which) makes it a priority to allocate the public cultural heritage as fully as possible to collective fruition".[7]

In this perspective, the core of this new face of public administration can be found in the impact that new technologies have had on cultural heritage, which guarantees the implementation of the cultural value through the globalization of content and digital fruition. The use of emerging technologies[8] - including Blockchain[9] - aims to create a new

la Costituzione, in *Rivista Giuridica dell'edilizia*, 1967, 7; E. Spagna Musso, *Lo Stato di cultura nella Costituzione italiana*, Naples, Morano, 1961, 73; E. Picozza, *Tutela e promozione dell'arte e della cultura. Relazione tenuta al Convegno annuale A.I.P.D.A. 2018 su: Arte, Cultura e ricerca scientifica – Costituzione e Amministrazione*, Reggio Calabria, 2018.

[3] For acute reflections on PNRR, see M. Clarich, *Il Pnrr tra diritto europeo e nazionale un tentativo di inquadramento giuridico*, in *AstridRassegna*, 2021, 1-15 and L. Casini, *Il ministero della Cultura di fronte al PNRR*, in *Aedon*, 2, 2021.

[4] "Indeed, what counts, in order to identify them, is the value they have (their cultural interest), an intrinsic value, which is always a human value, a value of civilization, which expresses the way of 'thinking, feeling and living of social groups in time and space": in these terms see V. Cerulli Irelli, *Beni culturali, diritti collettivi e proprietà pubblica*, in Vv. Aa., *Scritti in onore di Massimo Severo Giannini*, vol. I, Milan, Giuffrè, 1988, 140.

[5] These points were first highlighted by G. Rolla, *Beni culturali e funzione sociale*, in *Le regioni*, 1987, 57 and in Vv. Aa., *Scritti in onore di Massimo Severo Giannini*, vol. II, Milan, Giuffrè, 1988, 563.

[6] On the general concept of valorisation see P. Carpentieri, *Fruizione, valorizzazione, gestione dei beni culturali*, *Relazione al convegno "Il nuovo codice dei beni culturali e del paesaggio. Prospettive applicative*, 26 July 2004, who said on Article 9 "we move [...] from a static idea of protection, as a "state" reservation of the cultural property and as a limitation to its commercialisation and use, to a dynamic idea of the management of the cultural property, centred on the enhancement of the expression of its cultural value, which aims to become a service offered to the cultural growth of the public". See also L. Casini, *Valorizzazione e fruizione dei beni culturali*, in *Giornale di diritto amministrativo*, 5, 2004, 479; Id., *La valorizzazione dei beni culturali*, in *Rivista trimestrale di diritto pubblico*, 2001, 651 ; M.C. Cavallaro, *I beni culturali: tra tutela e valorizzazione economica*, in *Aedon*, 3, 2018; S. Cassese, *I beni culturali dalla tutela alla valorizzazione*, in *Giornale di diritto amministrativo*, 1998, 673 et. seq.; A. Iacopino, *Modelli e strumenti per la valorizzazione dei beni culturali. Spunto di riflessione nella prospettiva del risultato amministrativo*, Naples, Editoriale scientifica, 2017, *passim*; S. Mele, *Valorizzazione, fruizione ed uso dei beni culturali*, in *Il diritto dei beni culturali e del paesaggio*, E. Follieri (ed.), Naples, Edizioni Scientifiche Italiane, 2005, 271-303; F. Merusi, *Pubblico e privato e qualche dubbio di costituzionalità nello statuto dei beni culturali*, in *Diritto amministrativo*, 2007, 1; G. Severini, *Valorizzazione del patrimonio culturale*, in M.A. Sandulli (ed.), *Codice dei beni culturali e del paesaggio*, Milan, Giuffrè, 2012, 53; Id., *La valorizzazione dei beni culturali*, in *Rivista giuridica dell'ambiente*, 3, 2013, 238; A.L. Tarasco, *Diritto e gestione del patrimonio culturale*, Bari, Laterza, 2019.

[7] In these terms see N. Aicardi, *L'ordinamento amministrativo dei beni culturali. La sussidiarietà nella tutela e nella valorizzazione*, Turin, Giappichelli, 2002, 227.

[8] See A. Lazzaro, *Innovazione tecnologica e patrimonio culturale tra diffusione della cultura e regolamentazione*, in *www.federalismi.it*, issue 24, 20 December 2017, 2, especially 9. In her opinion, "there is no doubt that technologies for their enormous potential applied to cultural property, therefore, should be viewed favorably, appreciating their positive content, as they can contribute to the preservation of the cultural identity of places, the dissemination of culture and the production of new cultural offerings, and, they can be an important driver supporting competitive growth, as well as the development of innovative business models, with the advantage of diffusing knowledge of property without endangering its preservation or maintenance. [...] All this, from a socio-cultural point of view, helps to recover and pass on more easily to future generations the cultural identity of one's own country and in the same time encourages knowledge of other cultures". For an illustration of emerging and distributed ledger technologies see G. Gallone, Blockchain*, procedimenti amministrativi e prevenzione della corruzione*, in *Il diritto dell'economia*, 3, 2019, 187-212; Id., *La pubblica amministrazione alla prova dell'automazione contrattuale. Note in tema di* smart contracts, in *www.federalismi.it*, issue 20, 24 June 2020, 142-170; A.G. Orofino and G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giurisprudenza italiana*, 7, 2020, 1738-1748; A.G. Orofino, *La semplificazione digitale*, in *Il diritto dell'economia*, 3, 2019, 87.

[9] For a technical reconstruction of the Blockchain technology, see, furthermore, L. Parola, *Blockchain e contratti intelligenti: uno sguardo al mercato dell'energia*, in *Il teleriscaldamento, la Blockchain e i contratti intelligenti*, E. Bruti Liberati, M. De Focatiis and A. Travi (eds.), Padua, Wolters Kluwer, 2019, 93; F. Faini, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *www.federalismi.it*, issue 16, 27 May

connection between technology and cultural heritage, which, as a digital "fruition property",[10] is essential to pursue the objectives of the promotion and development of culture[11] that "the State [...] must ensure the community […] the enjoyment of the cultural values expressed by it".[12] In this context, firstly, the enhancement of cultural property must be carried out, considering its overall value in compliance with protection legislation,[13] and, secondly, every citizen can enjoy the cultural property (digital native or merely digitally transited) by accessing it with a personal account.[14] This strategy aims to create new or more up-to-date forms of protection to defend the integrity of cultural heritage, which combine guarantees for better collective enjoyment with protection for the benefits of future generations.

Massimo Severo Giannini's highly topical reflections fit into this renewed context. He said that "the cultural property is public not as property of ownership, but as property of enjoyment […] Universal usability is what is of legal interest".[15] Giannini's reconstruction stimulates a reinterpretation of the ultimate goal pursued by cultural heritage, also from a digital perspective, which reflects the provisions of the Council of Europe Framework Convention on the Value of Cultural Heritage for Society and the Recommendation concerning the Protection at national level of the cultural and natural heritage adopted by the General Conference of UNESCO on 16 November 1972.[16]

It is clear and uncontroversial that globalization and the recognition of a universal value of cultural heritage, combined with digital accessibility to it, complements a model characterized by a bottom-up approach that enables a direct approach to cultural heritage. This approach is an expression of a tendency to consider, as a priority, the side of the users of the digitalized cultural property. Specifically, the dialogue tool provided using artificial intelligence and distributed ledger

2020, 93; M. Faioli, E. Petrilli and D. Faioli, *Blockchain, contratti e lavoro. La ri-rivoluzione del digitale nel mondo produttivo e nella PA*, in *Economia e lavoro*, 2016, 139-158, especially 143; A.M. Gambino and C. Bomprezzi, *Blockchain e protezione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3, 2019, 625; F. Sarzana di S. Ippolito and M. Nicotra, *Diritto della Blockchain, intelligenza artificiale e IOT*, Milan, Wolters Kluwer, 2018.

[10] On this issue see P. Forte, *Il bene culturale pubblico digitalizzato. Note per uno studio giuridico*, in *P.A. Persona e Amministrazione*, 2, 2019, 245, especially 265. See also L.R. Perfetti, *Il bene pubblico ai tempi dell'assenza della cosa. Appunti per una possibile (contro)teoria dei beni pubblici*, in *P.A. Persona e Amministrazione*, 2, 2019, 303-310.

[11] For acute reflections on this point see P. Forte, *NFT, tutto il potenziale (reale) di ciò che presenta una "cosità"*, in *Il Mattino*, Naples, 2022, which says that "today's public museums are able to make a commitment on such advanced, and innovative fronts, accepting to experiment and, thus, helping themselves and all of us to understand, comprehend, practice the new possibilities of the digital dimension of cultural heritage. [...] we must recognise [...] the merit of having accepted these challenges, one of which consists in using elements of the heritage assigned to them to set up and circulate new tools called NFT, that is Non-fungible Token, which can be translated into Italian but risks being misleading, given that this acronym today designates a plurality of devices that have significantly different characteristics, but for what interests us have in common, at least, that they use a digitalised image of a cultural property and are made unique using a technological expedient. Not simply a copy and not even just a representation, but something else with its own original "cosità", which can provide them with a higher value than reproduction. [...] The Ministry of Culture set up a technical table to draw up behavioural guidelines to help the structures that protect, preserve and guarantee heritage (so that we can enjoy it) to handle them".

[12] See Italian Constitutional Court, 6 March 1990, no. 118, in *Foro italiano*, I, 1990, 1101

[13] On the globalization of cultural property see, *amplius*, L. Casini, *La globalizzazione dei beni culturali*, Bologna, Il Mulino, 2010, *passim*.

[14] See P. Carpentieri, *Tutela e valorizzazione dei beni culturali*, in *Urbanistica e appalti*, 9, 2003, 1019, "on the one hand, valorization means the realization of the conditions for the best fruition of the cultural property, i.e. for the best management of the property in order to ensure the maximum expression of its ontological vocation and destination for public fruition. On the other hand, a second, more economistic conception of the notion of *mise en valour* of the cultural property aims at considering valorization as a mode of entrepreneurial management of the cultural property able to determine (at least) sufficient revenue to (generally) cover management costs and to ensure a reinvestment useful for the strengthening and improvement of protection".

[15] See, in these terms, M.S. Giannini, *I beni culturali*, in *Rivista trimestrale di diritto pubblico*, 26/1, 1976, 24.

[16] A fundamental contribution is also due to UNESCO for the elaboration of the concept of "common heritage of mankind". On this point see, among others, J.H. Merryman, *Protection of the cultural heritage*, in *American Journal of Comparative Law*, 1990, 513; U. Leanza, *La protezione dei beni culturali e il concetto di patrimonio comune dell'umanità*, in *Scritti in onore di Angelo Falzea*, Milan, Giuffrè, 1991, I, 822; V. Pepe, *Il paesaggio naturale e culturale e il patrimonio mondiale dell'umanità*, in *Trattato di diritto amministrativo*, G. Santaniello (directed by), vol. XXXIII, A. Catelani and S. Cattaneo (eds.), *I beni e le attività culturali*, Padua, Cedam, 2003, 45; E. Baroncini (ed.), *Il diritto internazionale e la protezione del patrimonio culturale mondiale*, Bologna, Ams Acta, 2019; T. Scovazzi, *La Convenzione per la salvaguardia del patrimonio culturale intangibile*, in T. Scovazzi, B. Ubertazzi and L. Zagato (eds.), *Il patrimonio culturale intangibile nelle sue diverse dimensioni*, Milan, Giuffrè, 2012.

technologies is designed to include multiple social demands in public policies aimed at the protection and enhancement of cultural heritage.[17] This aims to build a connection between innovation and the virtual fruition of cultural property and consequently avoid the cultural inadequacy of museums or other cultural sites.[18]

The emphasis on fruition gets a strong accentuation, more recently, in the choices made with the PNRR: the Plan's exhibition process reveals the multiple skills of artificial intelligence[19] to introduce the public to culture and art using active enhancement tools.[20]

The Plan, in Mission 1 "Digitalisation, Innovation, Competitiveness, Culture and Tourism", offered the opportunity to act on the digital transformation by supporting the innovation of the production system and pressed on the need to invest in two key sectors, tourism and culture, aiming at reducing the structural gap in terms of competitiveness, productivity and digitalization of our country, in general, and of the Mezzogiorno, in particular. In this context, the Plan noted that emerging technologies, including Blockchain, are applicable as an important guide in the process of creating a Digital Cultural Heritage. In this process, digital platforms and strategies allow the exploration of new forms of protection, valorization and fruition of cultural heritage, as well as an easier accessibility and fruition of cultural property, as an instrument or object of culture, by removing the physical and cognitive barriers of museums, libraries and archives.[21]

The PNRR puts a strong accent on renewing the methods used for the fruition of cultural property and provides citizens a system that allows for better conservation of cultural property due to the collection and storage techniques adopted with the consequent guarantee of safe transmission to future generations.

The peculiarities of artificial intelligence concerning the traceability of operations and the application of the diffuse validation model, when appropriately included in the digital revolution of culture, make it possible to eliminate redundant data during the populating and cataloguing of cultural heritage, enable a new form of participation to transfer the entire cultural heritage on digital media, and allow the complexity of the cultural property[22] to be kept within focus by harmonizing different knowledge through interoperable language.

In order to encourage universal fruition of cultural heritage, digital systems in the cultural sector are therefore designed to achieve an accessible mapping of cultural heritage, fully digitized and ready to exploit the peculiarities of distributed ledger technologies, including Blockchain.

This is a digitalization process (for which a meritorious judgement must be reserved) that aims to transform cultural heritage into digital cognitive capital with diffuse accessibility and its potential, applied to the universal fruition

[17] See B. Barraud, *Les blockchains et le droit*, in *Revue Lamy droit de l'immatériel*, 147, 2018, 1. The Author says that: "Le futur quel les blockchains rendent possible est un monde plus horizontal. Le nouveau droit qu'elles forgent serait par conséquent un droit plus horizontal, se passant d'organes de tutelle et de contrôle […] les blockchains permettraient ainsi de reconstruire sur de nouvelles bases les sociétés, le collectif, les interindividualités, suivant le modèle d'une société décentralisée, horizontalisée".

[18] On this point see *Il patrimonio culturale per tutti. Fruibilità, riconoscibilità, accessibilità. Proposte, interventi, itinerari per l'accoglienza ai beni storico-artistici e alle strutture turistiche*, G. Cetorelli and M.R. Guido (eds.), Quaderni della valorizzazione – NS 4, Rome, 2017, 20.

[19] For an analysis of new risks for public administrations in the use of AI, see A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law – Erdal*, vol. 1, issue 1-2, 2020, 63-67. See, also, on the impact of Artificial Intelligence on Administrative Activity E. Picozza, *Politica, diritto amministrativo* and artificial intelligence, in *Giurisprudenza italiana*, 7, 2019, 1761-1771 and D.U. Galetta and J.G. Corvalán, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *www.federalismi.it*, issue 3, 6 February 2019, 2-23.

[20] Digitalization cannot be ignored, not only in terms of contents, but also in terms of modes of fruition and instruments for communicating and conveying the cultural offer. In this sense see A. Meschini, *Digital technology in the communication of Cultural Heritage. State of the art and potential development*, in *DisegnareCon – Scientific Journal on Architecture and Cultural Heritage*, 2011, 8.

[21] On this topic see, concurringly, V. Fanti, *Verso un turismo ecosostenibile e una digitalizzazione del patrimonio culturale*, in Vv. Aa., *Il Pnrr alla prova del Sud*, L. Bianchi and B. Caravita (eds.), Naples, Editoriale Scientifica, 2021, 137-146.

[22] First mention of the notion of cultural property was made in the *Convention pour la protection des biens culturels enc as de conflict armé* signed in 1954 in L'Aia. For the Convention Text see *Per la salvezza dei beni culturali in Italia. Atti e documenti della commissione d'indagine per la tutela e la valorizzazione del patrimonio storico, archeologico, artistico e del paesaggio*, Rome, Colombo, III, 1967, 59.

of cultural property, can support the preservation of the cultural identity of places, the circulation of culture and the creation of new cultural offers (just think about initiatives such as Aerariumchain, the MarTa 3.0 project, the ARTathlon contest, etc.).

In these choices, one can see the renewed need to provide for a new valorization of digitized cultural heritage and the necessity to set up new and more effective models for its fruition. And so in an organic system of digital revolution, the aid of strategies aimed at a useful distribution of data (Blockchain) allows the development of applications for the creation of a distributed archive to catalogue artworks held by museums and other cultural sites;[23] it enables the creation of new cultural content and the development of digital services by cultural/creative enterprises or start-ups; and, finally, it provides greater certainty and transparency on the origin and authenticity of the artworks by ensuring a control system on the originality and truthfulness of the cultural heritage.

A global fruition, even if digital, that becomes the aim both of the valorisation activity and of the protection of cultural property as set out in Articles 3 and 6, comma 1, of the Italian Cultural Heritage and Landscape Code.

3. *Some Observations on the Intangibility of Digital Cultural Heritage*

On the second line of research relating to the undoubted benefit of digital transition for the valorization of the "new" intangible cultural property, it is essential to underline the need, frequently remarked, to overcome the limit of materiality to achieve an "autonomous" digital dimension of the property. The cultural property gains World Heritage status regardless of its physical site or the virtual support in which it is located. The most important thing is how the property is conserved, enhanced and made useful.[24] In a digitally-oriented interpretation Massimo Severo Giannini sustained that: "the cultural property is not a material property, but an immaterial one: being a testimony having the value of civilization is an immaterial entity, which is related to one or more material entities, but legally it is distinct from them, in the way that they are a physical support, but not a juridical property". Cultural property's inherency to the thing is overcome as the cultural value of a property is an immaterial property not requiring identification with the thing to acquire culturality. These observations underline an overall standpoint which considers that digitalization of cultural heritage is the final step in a complex reform process aimed to affirm the intangible cultural value of cultural property.

These actions prompt further remarks.

In this digital-transition path are included the reflections flowing into the Italian Cultural Heritage and Landscape Code (Legislative Decree No. 42 of 22 January 2004), which in Article 2 aimed to overcome the "realness" of things included in cultural property to dwell, firstly, on the intangible value of cultural property seen as testimony having civilization value and, secondly, to accord relevance and protection to nonmaterial cultural property whose tangibility is excluded. The Code ensured this by including all cultural and landscape heritage with "cultural value" in the unitary class of cultural heritage. The Italian Cultural Heritage and Landscape Code demands the "memory" be protected as a prerequisite of national identity, not its tangible dimension.[25] So, although it can be agreed that the mere digital reproduction of the real cultural property is not, by itself, a "new" intangible cultural property, but rather a "new" way to benefit from it, it should also be noted that, in line with European policies, the protection of cultural heritage "also means promoting its regeneration, supporting contemporary creativity".[26]

[23] See, on the matter, B. Barraud, *Les blockchains et le droit*, 48, who said that a blockchain "could remind us (using a metaphor) the idea of a large, open, unforgeable account book, freely accessible and in which it is possible for everyone to write under the control of all, in the knowledge that all that has already been written is unchangeable. A page of a book would correspond to a block, while its binding would form the chain". See, also, O. Lasmoles, *La difficile appréhension des* blockchains *par le droit*, in *Revue internationale de droit économique*, 4, 2018, 453.

[24] From this point of view see L. Bobbio, *Le concezioni della politica dei beni culturali*, in Vv. Aa., *I beni culturali: istituzioni ed economia. Tavola rotonda nell'ambito della Conferenza annuale della Ricerca (Roma, 20 maggio 1998)*, Atti dei convegni Lincei, no. 152, Accademia dei Lincei, Rome, 1999, 13 et. seq.

[25] See L.R. Perfetti, *Premesse alle nozioni giuridiche di ambiente e paesaggio. Cose, beni, diritti e simboli*, in *Rivista giuridica dell'ambiente*, 1, 2009, 1.

[26] These words are from E. Sciacchitano, *Il patrimonio culturale nelle politiche e nei programmi dell'Unione europea. Ampliando l'orizzonte dalla conservazione all'innovazione*, in *Cartaditalia*, vol. II, 2018.

Similarly, the first reflections on the digital transition of cultural property should also be viewed from the perspective of the idea that the "new" digitalized property can be marked by unprecedented traits in relation to its analogue model[27] and, only in residual hypotheses, can be a simple copy of the basic tangible property.[28] This occurs in a reinterpretation of the notion of cultural heritage aimed at the valorization of immateriality[29] that draws its inspiration from the UNESCO charter for the Preservation of the Digital Heritage[30] and the Recommendation of 22 February 2017 on The European Cultural Heritage Strategy for the 21st Century.

Indeed, in these contexts there is a need to overcome the limitation of *res quae tangi potest* in the name of digital transition. We see the potential of the digital transition for the valorization of "new" immaterial cultural property in the relentless digitalization process that is investing our country.

The digital cultural property is perceived as a cognitive property, a provider of knowledge and "memory" to be protected, as a prerequisite of national identity and is not strictly related to tangibility. This is a property that can no more be said to be a simple reproduction of the original property, but which becomes richer with inscriptions in its digital "migration" precisely in order to avert a possible loss of cultural value, to provide new cognitive content and so acquire its own identity as an art object. Consequently, the protection of the "new" immaterial cultural property is seen in the provision of new forms of digital protection that preserve the immaterial value of the property and, therefore, its cultural value regardless of its material support.

In this direction, the aid of digital strategies, which can realise the recording of cultural property in a distributed archive, is oriented to using the algorithm, in support of the creation of a digitalized cultural property, as a technological infrastructure aimed at the reconstruction of the immaterial dimension of the basic analogue property. Indeed, it is

[27] A position radically opposed to the explicit prediction of new and autonomous immaterial cultural property can be found in P. Carpentieri, *Digitalizzazione, banche dati digitali e valorizzazione dei beni culturali*, in *Aedon*, 3, 2020, in which "[i]t is wrong to think that digital reproductions uploaded on the Internet constitute new, autonomous "immaterial cultural property". If anything, they are new "uses" of the intangible value contained in (and expressed by) the (tangible) cultural property. [...], it is not the "object" of the discipline that changes, but the "discipline" of the object (the discipline of a new possible use of it, carried out through an innovative medium, which complements the traditional ones). [...] digital reproductions of the cultural good are digital copies of the real cultural good (which is necessarily a *res corporalis*)".

[28] On this topic see, *amplius*, P. Forte, *Il bene culturale pubblico digitalizzato. Note per uno studio giuridico*, 256. In his opinion, "in order to try to identify the characteristics of a cultural property that has been digitalised, it may be tempting, first of all, to consider that digitalization basically consists in a simple reproduction, a function that has been widely known for a long time for cultural property; [...] and, secondly, that digitalization also has the possibility, in order to make up for the possible loss of "testimony" [...] of adding to the reproduction [...] a series of potentialities, that even in the most elementary operations allow, for example, a more accurate possibility of study, a multiplication and a deepening of perceptive experiences, but above all to provide contents and cognitive tools of various kinds, [...] that make up for what is lost with the lack of *cosità* and originality, the decrease of its aura, and increase the capacity to convey knowledge, thus bringing back and adding value". On the theme of the digital as a new form of cultural property, see also, D. Donati, *La digitalizzazione del patrimonio culturale. Caratteri strutturali e valore dei beni, tra disciplina amministrativa e tutela delle opere d'ingegno*, in *P.A. Persona e Amministrazione*, 2, 2019, 323-337.

[29] See S. Cassese, *I beni culturali da Bottai a Spadolini*, in *L'amministrazione dello Stato*, Milan, Giuffrè, 1976, 177, and Id., *Il futuro della disciplina dei beni culturali*, in *Giornale di diritto amministrativo*, 2012, 781; G. Morbidelli, *Dei beni culturali immateriali*, in Vv. Aa., *Scritti in onore di Ernesto Sticchi Damiani*, G. De Giorgi Cezzi, G. Greco, G. Morbidelli, P.L. Portaluri and F.G. Scoca (eds.), I, Naples, Edizioni Scientifiche Italiane, 2018, 580; Id., *Il valore immateriale dei beni culturali*, in *I beni immateriali tra regole privatistiche e pubblicistiche*, A. Bartolini, D. Ponti, G. Caforio (eds.), Naples, Jovene, 2014; L. Casini, *"Noli me tangere": i beni culturali tra materialità e immaterialità*, in *Aedon*, 2014, 1; E. Picozza and D. Siclari, *Per una (ri)costruzione dei patrimoni culturali immateriali*, in *www.federalismi.it*, issue 21, 13 November 2019.

[30] Article 1 of the Charter for the Preservation of Digital Heritage states that "the digital heritage consists of unique resources of human knowledge and expression. It embraces cultural, educational, scientific and administrative resources, as well as technical, legal, medical and other kinds of information created digitally, or converted into digital form from existing analogue resources. Where resources are "born digital", there is no other format but the digital object. Digital materials include texts, databases, still and moving images, audio, graphics, software and web pages, among a wide and growing range of formats. They are frequently ephemeral, and require purposeful production, maintenance and management to be retained. Many of these resources have lasting value and significance, and therefore constitute a heritage that should be protected and preserved for current and future generations. This ever-growing heritage may exist in any language, in any part of the world, and in any area of human knowledge or expression".

essential to clarify that this choice contributes "to the birth of a new epistemic, cognitive property, derived from the already-existing cultural property, but not identical, and not even simply reproductive"[31] and allows for the rebalancing of relations between the administration and citizens, by giving citizens the possibility of benefiting from the maximum fruition of cultural property.

4. *Some Concluding Remarks*

Overall, Italy's way facilitated a progressive and linear process of digital transition of cultural heritage that, starting with the digitalization of archival and book heritage, is gradually moving towards the implementation of advanced digital services, such as distributed ledger technologies, so that citizens gradually feel the benefits of the current transition.

The question on the table has multiple aspects that are relevant on different and concurrent levels. It cannot be denied that digitalization involves in some cases a simple reproduction of the original cultural property.[32] A digital replication of the tangible cultural property that represents a "new" way of enjoying it that stands alongside traditional ways and enriches the discipline of its protection, management and valorization. In this case, an inclusive approach re-emerges, aimed at including in the notion of cultural property[33] both the tangible and intangible and, consequently, the digital component.[34]

In other cases, the constitution of a digitalized cultural property using an algorithm reproposes all the complexity of the "real" cultural property and also aims to reconstruct the immaterial dimension of the basic analogue property in support of the creation of a technological infrastructure that reproduces it. The digitalized cultural property has no material evidence but, with the help of strategies able to implement the registration of data in a distributed archive, aims to become a digital "thing" with intangible cultural value. And so, the traceability of operations and the widespread validation model, when appropriately included in the digital revolution of culture, would eliminate redundant data, reduce accidental errors and episodes of abusive alteration, and contribute to the implementation of new forms of conservation, certification and fruition of cultural heritage.

[31] In these terms see P. Forte, *Il bene culturale pubblico digitalizzato. Note per uno studio giuridico*, 259.

[32] See L. Casini, *Riprodurre il patrimonio culturale? I "pieni" e i "vuoti" normative*, in *Aedon*, 3, 2018; M. Modolo, *Reinventare il patrimonio: il libero riuso dell'immagine digitale del bene culturale pubblico come leva di sviluppo nel post Covid*, in *Territori della Cultura*, 2020, 210; D. Manacorda, *Patrimonio culturale, libertà, democrazia. Pensieri sparsi di un archeologo incompetente a proposito di "Diritto e gestione del patrimonio culturale"*, in *Il capitale culturale. Studies on the Value of the Cultural Heritage*, 21, 2020, 15.

[33] The notion of cultural property is described by B. Cavallo, *La nozione di bene culturale tra mito e realtà: rilettura critica della prima dichiarazione della Commissione Franceschini*, in VV.AA.., *Scritti in onore di Massimo Severo Giannini*, 111-135.

[34] See on this topic P. Forte, *Il bene culturale pubblico digitalizzato. Note per uno studio giuridico*, 260. The Author thinks that "the real ambition of digitalization, in the cultural sphere, cannot be reduced to a mere duplication with a digital outcome, and to the care of the data consequently generated, since it can allow much more than a simple "representation", both for the wide possibilities of handling and creative alteration that even the simple digital image of an object allows, and for the availability of cognitive enrichment regarding a "thing" that its digital version allows to gather into a single entity".

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 233-239
ISSN 2724-5969 - ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 20

*The Conciliation Of Transparency Measures With the Processing of Possibly Sensitive Data by the Administration According to the French Administrative Judge**

Alexandre Lodie
(Doctor of International Law – Research Fellow at INRIA Grenoble)

French Council of State, Decision n. 431875, 10 June 2021

The publication, on the French Ministry of Economy and Finance's website, of a Civil servant's appointment order whose legal basis lies on a decree concerning the access of disabled persons to state functions constitutes a processing of data by automated means according to the Council of State. However, in judges' view, such processing cannot be seen as a processing of data "concerning health" pursuant to Article 9 of the GDPR.

ABSTRACT In this case, the plaintiff is a civil servant who has been appointed as Inspector of Finance according to a decree concerning the access of disabled persons to state functions. As provided by French Law, the appointment order – containing the legal basis of the nomination - was published on the Ministry of Economy and Finance's website. The claimant considered that the publication infringed his right to privacy and did not comply with the GDPR. In this decision, and contrary to what the Court of Appeal claimed, the Council of State concludes that the publication of the appointment order on the administration's website constitutes a processing of data by automated means and is thus subject to the GDPR. However, since the appointment order does not reveal the nature of the disability, nor its seriousness, the Conseil d'Etat considers that it does not constitute a processing of data concerning health. Such a decision seems to acknowledge a restrictive view of what constitutes "sensitive" data, which would not be in line with ECJ case law. Eventually, the Judges asked the administration to delete the mention of the decree in the appointment order as the appointment decision's period of appeal was over. Maintaining this information online was no longer necessary to achieve the purpose of the processing according to the French Administrative Judge.

1. *Introduction*

The free flow of data has become a central concern for the European market, as emphasised by the European Data Protection Supervisor (EDPS), Wojciech Wiewiorowski, who stated during the G7 DPA Roundtable in September 2022 that the "free flow of data is not only necessary to our digital economies and societies but even a precondition for a world placed under the auspices of cooperation and multilateralism".[1] This issue is related to the Big Data phenomenon which designates the inflation of data available online be they "generated from online transactions, emails, videos, audios, images, click streams, logs, posts, search queries, health records, social networking interactions, science data, sensors and mobile phone".[2]

Public administration and public bodies are no exception when it comes to processing and storing data. As such, they must be considered as a data-sharing stakeholder, hence the proposal on the European level of the Data Governance Act which aims "to address the barriers to a well-functioning data-driven economy and to create a Union-wide governance framework for data access and use, in particular regarding the re-use of certain types of data held by the public

* Article submitted to double blind peer review.
This work has been supported by the ANR 22-PECY-0002 IPOP (Interdisciplinary Project on Privacy) project of the Cybersecurity PEPR and by Inria action-exploratoire DATA4US.

[1] EDPS, *Data free flow with trust and international data spaces from an EU perspective*, G7 DPA Roundtable 2022, Bonn, 7 September 2022.

[2] S. Sagiroglu and D. Sinanc, *Big Data: A Review*, in *International conference on collaboration technologies and systems (CTS)*, Institute of Electrical and Electronics Engineers, 2013, 42.

sector".[3]

Besides, States and public administration are encouraged to publish their data to improve the transparency of the public life and decision-making processes, it is what some States call "open data" policies.[4] However, such a wide data disclosure might sometimes run contrary to individuals' data protection. This issue is all the more critical when sensitive data related to health, cultural or ethnic origin, political opinions, sexual orientation are at stake.[5]

The French Highest Administrative Court (Conseil d'État) released in 2021 a decision on the conciliation between the publication of administrative documents on the one hand and the protection of individuals' data, including sensitive data, on the other.[6]

In this case, a public agent had been nominated as Inspector of Finance by virtue of a decree bearing on the access of disabled persons to state functions.[7] The appointment order, mentioning the said decree, was consequently published on the website of the Ministry of Economy and Finance. The agent considered that such a publication constituted a violation of his private life and did not comply with the GDPR. He asked French administrative Courts to delete his name and date of birth from the appointment order. In front of their refusal, the case was brought to the Conseil d'État, which is the French Highest Administrative Court.

From this background the Conseil d'État had to settle several issues such as whether the publication of said appointment order constituted data processing by automated means subject to the GDPR. Then the Conseil d'État had to determine whether such processing could be seen as "data processing concerning health" as regards Article 9 of the GDPR.

This decision thus questions in a broader manner what can be considered as data processing by automated means, what sensitive data really are and how to conciliate the duty of the administration to publish administrative documents on the one hand with individuals' right to data protection on the other.

2. *A broad conception of "data processing" in accordance with the ECJ view*

One of the arguments put forward by the claimant was that the publication of the appointment order infringed European data protection law, including the GDPR. The problem was that the Appellate Court dismissed the application of the GDPR to the case since it claimed that "neither the publication by computerised means of a decree appointing public servants containing only the names of the persons concerned and an indication of the legal basis for their appointment, nor the decision refusing to put an end to this publication, could be regarded as relating to the processing of personal data by electronic means".[8] In other words, the Appellate Court considered that the publication of the appointment order did not constitute data processing, within the meaning of the GDPR.

The Conseil d'État however disapproved such a view, and repealed this decision by stating that "in rejecting the application of these rules, when the mere publication of personal data on a website is sufficient to make them applicable, the administrative court of appeal made an error of law".[9] The main issue was to consider whether the online publication of information regarding an individual could be considered as data processing.

By answering in the affirmative, the Conseil d'État seems to agree with the definition of data processing acknowledged by the European Court of Justice (ECJ). Indeed, in the Lindqvist decision, the ECJ considered that the publication of information related to an individual on a web page constituted data processing according to Article 3 of the

[3] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM (2020) 767 final, 25 November 2020.

[4] See Commission Nationale de l'Informatique et des Liberté (CNIL), *Publication en ligne et réutilisation des données publiques (« open data »),* available at: www.cnil.fr/fr/publication-en-ligne-et-reutilisation-des-donnees-publiques-open-data.

[5] See Article 9 of the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation).

[6] Conseil d'État, 10ème - 9ème chambres réunies, 10 June 2021, no. 431875.

[7] See Decree no. 95-979 of 25 August 1995, on the recruitment of disabled workers in the civil service, in application of article 27 of law no. 84-16 of 11 January 1984 on statutory provisions relating to the civil service.

[8] Conseil d'État, 10ème - 9ème chambres réunies, 10 June 2021, no. 431875.

[9] *Ibidem*.

GDPR.[10] More specifically the Court concluded that "the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means".[11] According to some scholars, following Article 3 of the GDPR, "any operation on the data constitutes a processing, especially as the list is merely illustrative"[12] which makes such a definition "particularly broad".[13] By concluding that the publication of an appointment order in this scenario was data processing subject to the GDPR the Council of State has therefore followed in the ECJ footsteps.

Another case law on the European stage tackled a similar issue. As a matter of fact, the ECJ, in its Google Spain decision released in 2014, used the same reasoning and concluded that "it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data'".[14] It should logically be acknowledged that "when Google does this on its own page, it is itself carrying out such processing since it collects, extracts, records, indexes and makes available the personal data of third-party sites".[15] Therefore, it can be deduced from ECJ case law that the mere publication of information related to an individual on a website or on search engines web pages constitute data processing subject to the GDPR.

To summarise, the French Conseil d'État, in its decision, adopts a similar approach to that of the ECJ, by considering that the publication of a civil servant's appointment order on the Ministry of Economy and Finance's website constitutes data processing by automated means which is regulated by the GDPR.

3. *A restrictive view of what constitutes a processing of "special categories of data"*

The claimant argued that the publication of the appointment order, mentioning the decree on the access of disabled persons to state functions violated his right to privacy. The processing of data related to the health status of a data subject is not only data processing subject to the GDPR, but also a processing of "special categories of data". However, the Conseil d'État surprisingly considered in this case that the administration did not process data concerning health, which questions what can be considered as processing of "special categories of data" revealing sensitive characteristics.

3.1. *A narrow interpretation of health data*

Once the Conseil d'État acknowledged that the GDPR applied, it had to determine whether such processing – which was indirectly revealing[16] the health status of the data subject – constituted a processing concerning health data.[17]

Health data is a category of data which is defined pretty broadly by EU data protection law as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".[18] For instance, in the Lindqvist case cited previously the ECJ claimed that "the expression data concerning health […] must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual"[19] and that "reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health".[20]

A semantic clarification must be made as a

[10] See ECJ, 6 November 2003, case C-101/01, *Bodil Lindqvist*.
[11] *Ibidem*, § 27.
[12] C. Castets-Renard, *La protection des données personnelles dans les relations internes à l'Union européenne*, in *Répertoire de droit européen*, Dalloz, Octobre 2018, § 22.
[13] *Ibidem.*
[14] ECJ, Grand Chamber, 13 May 2014, case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, § 27.
[15] M. Aubert, E. Broussy and H. Cassagnabère, *Chronique de jurisprudence de la CJUE: CJUE 13 Mai 2014, Google Spain SL, Google Inc. c Agencia Española de Protección de Datos, Mario Costeja González*, in *L'Actualité Juridique Droit Administratif,* 2014, 1147.
[16] S. Wachter and B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, no. 2, 2019, 563.
[17] See Article 9 of the GDPR.
[18] See Article 4 (15) of the GDPR.
[19] See ECJ, *Bodil Lindqvist*, note 10 above, § 50.
[20] *Ibidem*, § 51.

preamble: Article 9 makes a distinction between "processing of personal data revealing racial or ethnic origin, political opinions […]"[21] on the one hand and "data concerning health",[22] on the other. This distinction suggests that while an indirect connection between the processing and the nature of the data is enough to consider certain processing as processing of special categories of data, the connection must be direct when considering health data. However, this interpretation has been rejected by the ECJ which considered that "personal data concerning health should include all data pertaining to the health status of a data subject which "reveal" information relating to the past, current or future physical or mental health status of the data subject".[23]

Interestingly, the Conseil d'État does not reach the same conclusion at all, as it claims that "although the posting of such information online indirectly reveals that the persons recruited in this capacity suffer from a disability, it does not directly provide any information on the nature or seriousness of this disability and cannot therefore be regarded as processing data relating to the health of the persons concerned".[24] The degree of seriousness of a disability or an injury or the specificity of a disability are not relevant criteria as regards Article 9 of the GDPR, so such a statement by the Court can be a bit surprising.

The Court's reasoning does not seem to be consistent in the sense that it acknowledges that the processing involved indirectly reveals that the data subject suffers from a disability, but at the same time, it refuses to draw the right conclusion from this statement and to consider such a processing as a processing of "special categories of data" while the latter encompasses processing of data "pertaining to the health status"[25] of a data subject.

It is worth recalling that it is not the first time that the Conseil d'État makes the connection between the seriousness or nature of an injury or disability and the qualification of data as "data concerning health". For instance, in a decision which dates back from 2014, the Court stated that "the mention of the permanent incapacity rate or the disability rate of the "spouse or partner" and of the staff member's dependents is not data "relating to health" […] since it is not even alleged that it would provide information on the nature of the disability".[26] The Court concluded in the same manner as regards a file on education facilities which contained also information relating to care facilities where pupils can be enrolled.[27]

From a broader perspective this decision questions how to determine when data processing must be considered as processing bearing on "special categories of data".

3.2. *A decision in conflict with the European view on what constitutes "special categories of data"*

As mentioned previously the Conseil d'État adopted a quite narrow definition of what "health data" are while this category refers to "special categories" of data which benefit from additional protections under the GDPR.[28]

Very few case law are related to the specific issue of which data can be considered as "indirectly revealing" sensitive characteristics and thus as "special categories" of data. Furthermore, none of them – to our knowledge – refers to data revealing the health status of a data subject. However, it is worth analysing what the ECJ and data protection authorities throughout the EU have stated as regards data revealing sensitive characteristics, although such case law do not bear on health data.

The ECJ got referred lately for a preliminary ruling, in a case involving transparency measures required by the administration on the one hand and sensitive data protection issues on the other. The question that the Court had to settle was thus pretty similar to the Conseil d'État's, although not bearing on health data but on other sensitive data provided for by Article 9 of the GDPR.

In this case, the director of a Lithuanian public body had to release a declaration of interest containing several personal information about him and his partner, which

[21] See Article 9 of the GDPR.
[22] *Ibidem*.
[23] ECJ, Grand Chamber, 1 August 2022, case C-184/20, *OT v Vyriausioji tarnybinės etikos komisija*, § 124.
[24] Conseil d'État, 10ème - 9ème chambres réunies, 10 June 2021, no. 431875.
[25] See Recital 35 of the GDPR.
[26] Conseil d'État, 10ème / 9ème sous-sections réunies, 28 March 2014, no. 36104.
[27] Conseil d'État, 10ème et 9ème sous-sections réunies, 19 July 2010, no. 334014.
[28] See Article 9 of the GDPR.

was likely to reveal at least some sensitive characteristics, such as his sexual orientation.[29] Said declaration of interest was intended to be published, as required by Lithuanian Law. The ECJ had therefore to determine whether such data processing could be considered as a processing of sensitive data.

The ECJ concluded that "the publication, on the website of the public authority responsible for collecting and checking the content of declarations of private interests, of personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data".[30] Even though the processing was not directly related to the sexual orientation of the data subjects the ECJ considered that it was a processing of special categories of data.

The ECJ, in its decision, does not make any relationship between the nature or specificity of sensitive characteristics and the nature of the data processing as "sensitive", lying in the scope of Article 9 of the GDPR. It is also possible to consider that the ECJ, in the above-mentioned Lithuanian use case[31] reached this conclusion because the information contained in the declaration of interest was revealing a specific sexual orientation, but such an interpretation would be far-fetched since the Court does not say anything on this specific point.

The decision of the Conseil d'État was released one year earlier, so it could not foresee what the ECJ would have stated in such a situation. However, one could have expected the Conseil d'État to follow a similar reasoning to that of the ECJ even though the nature of the data concerned was not exactly the same.

In any case, the view expressed by the Conseil d'État is likely to limit strongly the scope of Article 9 of the GDPR and the protection of individuals' sensitive characteristics. Such a restrictive view is all the more surprising that, in any case, the administration could have relied upon the "substantial public interest"[32] exception. In other words, even if the Conseil d'État had acknowledged that the online publication of an appointment order containing sensitive information constituted a processing of "special categories of data", French administration would have possibly been able to carry out such processing since the publication of civil servants' appointment orders is mandatory under French Law and possibly serves a substantial public interest. The judges interestingly mention the exception of substantial public interest by citing the GDPR, without further explanation. It suggests that the administration could possibly rely on this exception.

To summarise, the Conseil d'État adopts a restrictive view of what constitutes processing of data concerning health, claiming that the sensitive nature of the data (and consequent processing) depends on the specificity and seriousness of the disability.

It is worth noting that the Norwegian DPA also had to address a similar issue and adopted a view which can be considered as the opposite of the Conseil d'État's reasoning on whether data need to be precise to be considered as data of a sensitive nature.

In this case the data protection authority had to determine whether a dating app for LGBTQI+ people processes data of a sensitive nature by revealing data subjects' sexual orientation. The Norwegian Datatilsynet claimed that "being a Grindr user strongly indicates, and appears in most cases to accurately reflect, that the data subject belongs to a sexual minority. […] As established above, the wording of Article 9 does not require a revealing of a particular "sexual orientation", and the purpose behind Article 9 discourages a narrow interpretation".[33]

Even though this use case does not deal with data concerning health, it bears on the interpretation of what processing of "special categories of data" actually is. According to the Norwegian DPA, Article 9 of the GDPR must be interpreted in a broad manner, which indicates that the processing does not need to reveal a specific sexual orientation to be considered as processing of sensitive data.[34] In particular the company argued for its defense that everyone can subscribe to its services and not only LGBTQI+ people, so that the fact of being a Grindr user is not an indication of the

[29] ECJ, Grand Chamber, 1 August 2022, case C-184/20, *OT v Vyriausioji tarnybinės etikos komisija*.
[30] *Ibidem*.
[31] *Ibidem*.
[32] See Article 9 of the GDPR.
[33] See Datatilsynet, 13 December 2021, 20/02136-18, *Administrative fine - Grindr LLC*.
[34] *Ibidem*.

user's specific sexual orientation. Despite this argument, the DPA concluded that the use of Grindr was a strong indication of one's sexual orientation, which means that it is reasonable to think that a Grindr's user belongs to a sexual minority.[35] In this case the sensitive characteristic is deduced and not specific, but the Datatilsynet still claimed that it was enough to consider the processing as processing of "special categories of data".

The debate on how specific data must be to qualify their processing as processing of sensitive data remains open. For instance, the EDPB claims, considering the relation between video devices and sensitive data, that "video footage showing a data subject wearing glasses or using a wheel chair are not per se considered to be special categories of personal data".[36] However, the processing of a video stream showing a person who suffers from a disability would logically be seen as data concerning their health status. On the other hand, it would be impossible to acknowledge such an extreme view since almost every data processing would be qualified as processing of sensitive data.

Whereas the Conseil d'État stated that the seriousness and the nature of an injury were decisive factors to consider whether data are of sensitive nature, the Norwegian DPA claimed that a piece of information does not need to reveal a specific sexual orientation to be qualified as "sensitive". From this background it can be concluded that it can be hard to set the bar as whether data reveal sensitive features and thus, whether their processing should be considered as prohibited according to Article 9 of the GDPR.

Eventually, the processing was deemed unlawful by the Conseil d'État on other grounds such as non-compliance with proportionality and data minimisation principles.

4. *The unlawfulness of such a processing under necessity, proportionality and data minimisation principles*

Even though the Conseil d'État concluded that the publication of an appointment order mentioning a decree on the access of disabled persons to state functions could not be seen as a processing of data concerning health, it eventually claims that such processing was unlawful because of the way the processing was carried out. In particular, judges consider that "the permanent display of these personal data on the Ministry's website exceeds what is necessary in view of the purposes of the processing in question, which are to guarantee the rights of third parties and respect for the principle of equal access to public employment as set out in Article 6 of the 1789 Declaration of Human and Citizens' rights".[37] The proposed solution was to delete the legal basis of the appointment order once the latter's period of appeal expired.[38] This dictum is meant to strike a balance between data subjects' data protection rights and privacy on the one hand and the administration's duty to publish appointment orders on the other.

This view is in line with the ECJ's case law. Indeed, in the Lithuanian case cited above[39] the ECJ considered that "it must be found that the online publication of the majority of the personal data contained in the declaration of private interests of any head of an establishment receiving public funds, such as that at issue in the main proceedings, does not meet the requirements of a proper balance".[40]

In other words, the existence of a legal requirement concerning the data processing and the narrow definition of the concept of "data concerning health" would have implied that the individuals' protection was reduced, but these factors are not sufficient to consider that data processing is lawful. Indeed, the Conseil d'État concludes in this case that although the administration did not carry out a processing of sensitive data, it was not necessary to keep data online after the period of appeal was over.

5. *Conclusion*

In view of the above, it is worth noting that there is a pressing need to determine what constitutes processing of special categories of data, pursuant to Article 9 of the GDPR. There is indeed a wide array of data processing which can indirectly reveal some sensitive

[35] *Ibidem*.
[36] EDPB, *Guidelines 3/2019 on processing of personal data through video devices*, 29 January 2020, 17, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.
[37] Conseil d'État, 10ème - 9ème chambres réunies, 10 June 2021, no. 431875.
[38] *Ibidem*.
[39] See ECJ, Grand Chamber, 1 August 2022, case C-184/20, *OT v Vyriausioji tarnybinės etikos komisija*.
[40] *Ibidem*.

characteristics of a data subject. The question as to whether these processing must be considered as processing of sensitive data is largely debated, as the decision of French Conseil d'État illustrates. Indeed, the Conseil d'État seems to consider that only processing revealing the seriousness or the nature of a disability must be considered as processing of data concerning health. This view can be problematic since it runs contrary to the way the ECJ interprets the processing of health data and more broadly, to the way some DPAs interpret the processing of data likely to reveal sensitive characteristics.[41] This question is very critical since the development of machine learning technology enables the inference of sensitive characteristics from data which are not inherently sensitive.[42] One of the most relevant criteria to consider whether a processing of personal data can be considered as an unlawful processing of sensitive data is the purpose criterion. In other words, while the processing of data likely to reveal in an indirect fashion some sensitive data can be deemed lawful, the processing of said data with the intent to reveal sensitive characteristics should be deemed unlawful in whatever circumstances. For instance, the Information Commissioner's Office (ICO) claimed in the Cambridge Analytica use case that "since CA used the information collected to make predictions about data subjects' political affiliations and opinions, it is clear that the data should be considered sensitive personal data".[43] The link is thus drawn between the intent (purpose) and the qualification of a processing as revealing sensitive data. Further research should be undertaken on the topic of data processing indirectly revealing sensitive data through inferences.

[41] See Datatilsynet, 13 December 2021, 20/02136-18, *Administrative fine - Grindr LLC*.
[42] Article 29 Data Protection Working Party, *Advice paper on special categories of data ("sensitive data")*, Ref. Ares (2011) 444105, 20 April 2011, 6.
[43] ICO, *Investigation into the use of data analytics in political campaigns. A report to Parliament*, 6 November 2018, 36.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 241-265
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 21

National Reports

EUROPEAN UNION
edited by
Andrea CIRCOLO, Ph.D. in EU Law, University of Naples Parthenope
Angelo CORRERA, Ph.D. in EU Law, University of Naples Parthenope

NEW INTEROPERABLE EUROPE ACT TO DELIVER MORE EFFICIENT PUBLIC SERVICES THROUGH IMPROVED COOPERATION BETWEEN NATIONAL ADMINISTRATIONS ON DATA EXCHANGES AND IT SOLUTIONS

Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)

The European Commission has proposed a Regulation on the interoperability among public sector entities across the EU.

The European Commission has published the legislative proposal known as the Interoperable Europe Act, along with its accompanying Communication (18 November 2022).

The initiative aims to enhance collaboration and interoperability among public-sector entities across the European Union. The Act's main goal is to establish a network of interconnected digital public administrations that are, at the same time, independent and linked to each other. This effort will expedite the digital transformation of the public sector in Europe and contribute to the provision of improved public services to individuals and businesses.

Indeed, the digitization of public administrations is a key focus for this decade, and Member States are heavily investing in modernizing their public sector through digital means. However, despite the increasing number of digital services offered by the EU public sector, there is still a lack of adequate interoperability among them. In this regard, it is written down in the proposal that the Commission can 'set up projects to support public-sector bodies in the digital implementation of Union policies ensuring the cross-border interoperability of network and information systems which are used to provide or manage public services to be delivered or managed electronically ("policy implementation support project") (Art. 9, para 1).

By achieving these objectives, the Act plays a crucial role in attaining Europe's digital targets for 2030 and facilitating the smooth flow of trusted data. Additionally, implementing cross-border interoperability has the potential to generate significant cost savings. It is estimated that citizens could save between €5.5 and €6.3 million, while businesses engaged in transactions with public administrations could save between €5.7 and €19.2 billion.

From a first reading of the proposal, two possible advantages can already be pointed out:
a) The proposal backs the establishment of a governance model for this policy, comprising two principal entities - the Interoperable Europe Board and the Interoperable Europe Community;
b) The Act includes provisions for developing experimental solutions that facilitate collaborations between the public sector and innovative-technology companies and startups. The aim is to foster the creation of pioneering experimental solutions that can be implemented and shared across public services.

EUROPEAN DIGITAL IDENTITY (EID)

European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe

The revised Regulation seeks to guarantee universal access to secure and reliable electronic identification and authentication for individuals and businesses. This will be achieved through the use of a personal digital wallet on a mobile phone.

The Council has approved its common position on the proposed legislation concerning the framework for a European digital identity (so called 'general approach' – 6 December 2022).

In June 2021, the Commission put forth a framework for a European digital identity (eID), aiming to provide access to all EU citizens, residents, and businesses through a European digital-identity wallet (Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity - COM(2021) 281 final, 2021/0136(COD) – 3 June 2021, available on:

eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281.

The proposed framework entails modifications to the 2014 Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). The eIDAS regulation established the groundwork for secure access to public services and online transactions within the EU, both domestically and across borders.

The Council welcomed the EC's proposal to amend the eIDAS Regulation, as the revision aims to adapt the existing legal act to meet current market requirements. The Council stated the necessity to enhance digital-service solutions, ensuring broader access for both private and public sectors, as the goal is to make these solutions accessible to a significant majority of European citizens and residents. Indeed, the revision intends to achieve that at least 80% of European citizens should be able to use a digital ID solution to access key public services by 2030.

The ball is now in the European Parliament's court.

The hope is that, in the final draft, effective data protection will be looked at in the context of the protection of fundamental rights, in particular the right to privacy and the right to the protection of personal data, as already underlined Opinion of the European Economic and Social Committee on the proposal (COM(2021) 281 final – 2021/0136 (COD) – 20 October 2021, available on: eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021AE2756.

Indeed, the digitalization process, particularly the development of large-scale systems that store and process data, raises numerous security concerns regarding the vulnerability to fraud and data loss. Currently, e.g., there is no security system capable of providing comprehensive data protection. In light of this, the EESC already emphasized that users of European Digital Identity Wallets should be provided with assurance of compensation in the event of any adverse situations concerning their data, such as data theft or unauthorized disclosure. This liability should be strict, i.e. independent of whether the service provider is at fault.

THE COURT OF JUSTICE DECLARES A PROVISION OF THE ANTI-MONEY LAUNDERING DIRECTIVE INVALID FOR BEING CONTRARY TO THE CHARTER OF FUNDAMENTAL RIGHTS

Court of Justice of the European Union (CJEU) (Grand Chamber), Judgment of 22th November 2022, Joined Case C-37/20 e C-601/20, WM Sovim and SA v. Luxembourg Business Registers - Request for a preliminary ruling under Article 267 TFEU from the Tribunal d'arrondissement de Luxembourg, made by decision of 24 January 2020.

The Court of Justice declared invalid, in light of the Charter, the provision of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, pursuant to which Member States shall ensure that information on the beneficial ownership of companies and other legal entities incorporated in their territory is accessible to the public in all cases. In the Court's view, public access to beneficial-ownership information constitutes a serious interference with the fundamental rights to respect for private life and the protection of personal data, respectively enshrined in Articles 7 and 8 of the Charter. Indeed, the information disclosed allows a potentially unlimited number of persons to find out about the beneficial owner's material and financial situation. Moreover, the potential consequences for the persons concerned of any misuse of their personal data are aggravated by the fact that, once made available to the public, such data may not only be freely accessed, but also stored and disseminated.

Two appeals were brought to the EU Court of Justice by a Luxembourg company and the beneficial owner of a Luxembourg company, respectively, who had unsuccessfully requested the LBR to restrict public access to information about them. The two companies considered that the disclosure of that information was likely to entail a disproportionate risk of infringement of the fundamental rights of the beneficial owners concerned, and therefore, the court referred a number of questions to the Court of Justice for a preliminary ruling concerning the interpretation of certain provisions of the Anti-Money Laundering Directive and the validity of those provisions in light of the Charter of Fundamental Rights of the European Union.

It should be pointed out, that in accordance with the Anti-Money Laundering Directive, a Luxembourg law adopted in 2019 established a Register of Beneficial Owners, providing that a whole range of information on the beneficial ownership of registered entities must be recorded and stored therein. Part of this information is accessible to the public, in particular via the Inter-

net. That law also provides for the possibility for a beneficial owner to request the Luxembourg Business Registers (LBR), the manager of the Register, to restrict access to that information in certain cases.

In its judgment, the Court of Justice declares that the provision of the Anti-Money Laundering Directive under which Member States shall ensure that information on the beneficial ownership of companies and other legal entities incorporated in their territory is accessible to the public in all cases infringes upon the Charter.

In the Court's view, public access to beneficial ownership information constitutes a serious interference with the fundamental rights of respect for private life and of protection of personal data, enshrined respectively in Articles 7 and 8 of the Charter. Indeed, the information disclosed allows a potentially unlimited number of persons to find out about the beneficial owner's material and financial situation. Moreover, the potential consequences for the persons concerned of any misuse of their personal data are aggravated by the fact that, once they have been made available to the public, those data may not only be freely consulted, but also stored and disseminated.

The Court notes that the European Union legislature seeks to prevent money laundering and terrorist financing by establishing, by means of greater transparency, an environment less likely to be used for such purposes.

However, the Court finds that the interference resulting from such a measure is neither limited to what is strictly necessary nor proportionate to the objective pursued. In addition to the fact that the provisions at issue in the present case authorise the making available to the public of data which are neither sufficiently defined nor identifiable, the regime introduced by the anti-money laundering directive represents a considerably more serious infringement of the fundamental rights guaranteed by Articles 7 and 8 of the Charter than the previous regime, which provided not only access by the competent authorities and certain entities, but also by any person or organisation that could demonstrate a legitimate interest, aggravation that, however, did not result in any benefits from the new regime as compared with the previous one, from the point of view of the effectiveness of the fight against money laundering and the financing of terrorism.

In particular, the possible existence of difficulties in defining precisely the cases and conditions in which such a legitimate interest exists, relied on by the Commission, cannot justify the fact that the European Union legislature provides for public access to the information in question. The Court adds that the optional provisions enabling the Member States, respectively, to make the provision of beneficial-ownership information subject to online registration and to provide, in exceptional circumstances, for certain exceptions to public access to that information, are not, in themselves, capable of demonstrating either a proper balance between the public-interest objective pursued and the fundamental rights enshrined in Articles 7 and 8 of the Charter or the existence of sufficient safeguards enabling the persons concerned to effectively protect their personal data against the risks of abuse.

DATA RETENTION: TRAFFIC DATA OF ELECTRONIC COMMUNICATIONS FOR CRIME-PREVENTION PURPOSES

Court of Justice of the European Union (CJEU) (Grand Chamber), Judgment of 20th September 2022, Joined Case C-339/20 e C-397/20, VD and SR - Request for a preliminary ruling under Article 267 TFEU from the Cour de cassation - France, made by decision of 1st April 2020.

The Court of justice confirms the "prohibition of generalised and indiscriminate retention" of traffic data of electronic communications for crime-prevention purposes.

In its judgment, the Court was prompted by a reference for a preliminary ruling from the French Court of Cassation, in a case concerning the acquisition - in the context of criminal proceedings for the offences of insider dealing, secondary insider dealing, aiding and abetting, bribery and money laundering - of traffic data retained, for one year, on the basis of the relevant national legislation. The questions raised by the French Court of Cassation concerned, in particular

- the interpretation of the "market abuse" directive and regulation (Article 12(2)(a) and (d), Directive 2003/6/EC and Article 23(2)(g) and (h), Regulation (EU) 596/2014), read in conjunction with Article 15(1) of Directive 2002/58/EC, read in light of the Cdfue and the compatibility, with that framework, of national legislative measures imposing on operators of electronic communication services, a generalised, preventive and indiscriminate retention of traffic data for one year from the day of registration, for the purpose of combating market-abuse offences;
- the admissibility of the provisional effectiveness of domestic legislation, where deemed in-

compatible with European rules, in order to avoid excessive legal uncertainty and to allow the use, for evidentiary purposes, of data retained under such legislation.

Pending the decision of the Court of Justice, moreover, the Conseil d'État (French Data Network and others: nos. 393099, 394922, 397844, 397851, 424717, 424718), by which the national provisions on the generalised retention of connection data for the purposes of justice were declared unlawful, with the exception of the part relating to the retention of IP addresses and data relating to the personal identity of users of electronic communications networks, in line with the CJEU judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

With the VD judgment, the Court of Justice today declares incompatible with Article 15(1) of Directive 2002/58, read in light of Articles 7, 8, 11 and 52(1) CDFUE, national legislation, such as that at issue, which requires operators of electronic-communications services -for the purpose of combating market-abuse offences- to store the traffic data of all users of electronic communications media in a generalised and indiscriminate manner, 'without any distinction being made in that regard or any exceptions being provided for and without the required relationship, within the meaning of the case-law cited in the preceding paragraph, between the data to be retained and the objective pursued being demonstrated' (paragraph 94). The reference to the previous case law (and, in particular, to the judgment of 5 April 2022) therefore serves to reiterate, albeit indirectly, the parameters for the admissibility of the retention of printouts outlined there, i.e. subjective, geographical or other criteria (provided that they are objective and non-discriminatory) such as to imply a functional relationship between the investigative needs and the data to be acquired.

The Court reiterates, moreover, the inadmissibility of a limitation, in time, of a declaration of invalidity of domestic legislation requiring operators of electronic communications services to retain traffic data generally and indiscriminately and permitting them to be communicated to the competent authority without prior authorisation by a court or an independent administrative authority. Otherwise, the primacy and the need for uniform application of Union law would be undermined.

To quote from the judgment of 2 March 2021, H.K. v. Prokuratuur (C 746-18), the Court further states that the question of the admissibility of evidence obtained pursuant to national legal provisions incompatible with European Union law is a matter of national competence, in accordance with the principle of the procedural autonomy of the Member States, subject, however, to compliance with the principles of equivalence and effectiveness.

With regard to the latter principle, the Court points out that it requires the national court to exclude information and evidence obtained through the generalised and indiscriminate retention of traffic data and location data on the basis of rules incompatible with European Union law, or even through access by the competent authority to such data which is incompatible with European law, where the party against whom that evidence is used cannot 'effectively make its views known on that information and that evidence, which relates to a matter outside the knowledge of the courts and is capable of having a predominant influence on the assessment of the facts' (paragraph 106).

BELGIUM

edited by
Elise DEGRAVE, Professor at University of Namur; Director of research at NADI-CRIDS
Florian JACQUES, teaching assistant at University of Namur and researcher at NADI-CRIDS
Julie MONT, teaching assistant at University of Namur, researcher at NADI-CRIDS and lawyer at Namur Bar
Kathryn BARETTE, researcher at NADI-CRIDS

DATA PROCESSING BY PUBLIC AUTHORITIES

Belgian Data Protection Authority (BDPA) (Litigation chamber), decision 115/2022 of 19 July 2022

The BDPA had to rule on the question of whether the GDPR allows disclosure of sensitive data during a work meeting.

The BDPA received a complaint concerning the disclosure of personal data relating to an employee's health by her manager during a departmental meeting in which she was not present. First, the contentious chamber identified the data processing in question and recalled that oral communications do not fall within the scope of the GDPR. However, in the case at hand, the oral statements made by the manager were recorded

in the minutes of the meeting. Hence, a data processing under articles 2.1. and 4.1. of the GDPR took place. The decision also confirms that the disclosure of information relating to the claimant constitutes a processing of data relating to health. Second, the BDPA recalled that each processing operation must be based on one of the grounds of lawfulness enshrined in article 6.1. GDPR. Furthermore, as that the defendant processed data relating to the claimant's health, this processing must be based on Article 9.2. of the GDPR read in conjunction with Article 6.1. of the GDPR. In this case, the claimant's complaint was directed against the further processing (i.e the communication during a meeting) of information relating to her health. The litigation chamber decided that, even if the purposes for which the data were originally collected are identified, lawful and legitimate their further disclosure is not compatible with these purposes. Since the defendant is a public authority in respect of whom administrative fines cannot not be imposed the BDPA decided to issue a reprimand.

Brussels Court of Appeal, Brussels Markets Court, 19th Chamber A, judgment of 26 October 2022

An appeal was filed against the decision 31/2022 of 4 March 2022 (already commented in the previous report) of the Belgian Data Protection Authority.

The appealed decision concerned a case in which the claimant had been issued with a parking ticket and subsequently a parking charge. Until 1 January 2020, an autonomous entity of the city of Kortrijk called "the RCO" was authorised to process the vehicles plate number of offenders on the basis of a normative text ("deliberation no. 02/2016"). On 1 January 2020, this entity was dissolved and the city of Kortrijk took over this prerogative. The claimant therefore argued that the city of Kortrijk breached the GDPR when it relied on "deliberation 02/2016" to process his number plate. Unlike the RCO, the city was not the addressee of this normative text. Hence, according to the claimant, at the time of the facts, the City of Kortrijk was not authorised to perform the data processing necessary to identify his vehicle plate number. The City of Kortrijk argued that it was the legal successor of the RCO and was therefore authorised to process the complainant's personal data. The BDPA had considered that a legal succession could take place as long as the purpose of the processing of personal data remained unchanged. The BDPA also found that the city breached GDPR transparency and information requirements. During the appeal, the City (supported by the Federal Public Service Mobility) argued that during the procedure before the BDPA, (1) it was never informed of the exact offences it was accused of and (2) it was never clear against which arguments it could defend itself. In particular, the City argued that it had never been informed that it had breached the transparency requirements under the GDPR (arts. 5.1.a., 12.1. and 14.1.). According to the BDPA, this breach was indeed raised during the proceedings before the litigation chamber. In the Court's view, the elements on which the BDPA relied to allege that the breach of the duty of transparency could be imputed to the City of Kortrijk were not sufficient and that the latter should have been clearly informed of the legal bases on which the BDPA based the breach of its duty of transparency. The Court decided that the BDPA's decision was incompatible with the principles of diligence and fairness, the right to be heard and the right to cross-examine. It therefore ordered the BDPA to review the complaint against the City.

Council of State, judgment 254.571 of 21 September 2022

The Council of State received two actions for annulment of the Brussels regional government's decrees creating low emission zones (LEZ). The citizen who filed the claims relied, among others, on an argument based on the violation of the GDPR.

A citizen filed, before the Council of State, two actions for annulment against the decrees of the Government of the Brussels-Capital Region establishing low emission zones. Adoption of these decrees stems from the Directive 2008/50/EC, which requires Member States to establish zones in which ambient air quality is assessed and to define Low Emission Zones. This implies that access to certain categories of vehicles that emit atmospheric pollutants is restricted in LEZ. The government can however waive the restriction by granting temporary access to the LEZ against payment. Before the Council of State, one of the arguments raised by the applicant is that the government's request to communicate the identity of the driver upon purchase of a LEZ pass, violates the GDPR (art. 5.1 c.). To that extent, the applicant considered that only processing of vehicle plate number was relevant to purchase a pass. On the other hand, other data collected (identity of the driver, identity of the applicant for the pass) were not necessary and were therefore violating the right to privacy.

The Council of State did not follow this argument. On the contrary, the decision highlights that there is no requirement that the purchaser of the pass correspond to the person who will use the vehicle covered by the pass. According to the Council of State, the requirement to state one's identity is a purely formal requirement common to any request filed before an administrative authority. Hence, this data processing does not disproportionately infringe the right to privacy.

Belgian Data Protection Authority (BDPA) (Litigation chamber), decision 186/2022 of 19 December 2022

Two complaints were filed for the disclosure of personal data by the Financial Services and Markets authority (FSMA).

The BDPA received complaints regarding a payment-reminder email sent by the FSMA (the defendant). In particular, this email was sent to the claimants and to several hundred other recipients with the email addresses visible in CC (Carbon Copy) instead of CCC (Carbon Copy Invisible). In this case, the BDPA didn't assessed the lawfulness ground of the processing of the complainants' email addresses as it was not the subject of the complaint. In addition, two arguments were put forward by the defendant. First, it was a regrettable individual error made by an employee. Second, the email did not contain any personal data (including sensitive data) since the only information disclosed to the recipients was the email addresses of the other recipients. The defendant also indicated that various protection measures had been taken within the FSMA in order to comply as much as possible with the GDPR (e.g. appointing a DPO and organising training courses in data protection for the employees). In the decision, the litigation chamber recalls articles 24.1, 25 and 74 of the GDPR relating to the rights and duties of the controller as well as the latter's accountability. The BDPA found that the defendant had failed to comply with these articles because, as a controller, it had not taken the appropriate technical and organisational measures to ensure and be able to demonstrate that processing at hand was compliant the GDPR. Therefore, the authority decided to issue a reprimand.

RIGHT TO ERASURE – RIGHT TO BE FORGOTTEN

Brussels Court of Appeal, Brussels Markets Court, 19th Chamber A, judgment of 26 October 2022

An appeal was lodged against the decision taken by the BDPA on 17 March 2022 (decision 38/2022 already commented in the previous report).

The appeal concerned a rejected-complaint filed by a lawyer to whom Google had refused dereference in various press articles reporting the lawyer's previous convictions and subsequent disbarment. The BDPA below nevertheless issued a reprimand to Google Belgium for non-compliance with articles 12.1, 12.2 and 17 of the GDPR. Google Belgium and Google LLC (the claimants) are also appealing the BDPA's decision with regard to this reprimand. According to the claimants, the authority violated the provisions of the GDPR in that it found an infringement of the Regulation and issued the related penalty to a local establishment of Google LLC (i.e Google Belgium) whereas it also acknowledged that Google LLC, being the controller, is the one bound to comply with the infringed rules. The claimants also appealed the BDPA's decision for alleged lack of reasoning . In particular, they challenged the fact that the appealed decision was referring to one of the BDPA's decisions (decision no. 37/2020) which has since been annulled by the Market Court. The Market Court followed this argument, considering that the illegality of decision no. 37/2020, to which the BDPA referred in order to impose the sanction against Google Belgium, justified the annulment of this sanction. The Court considers that a "motivation by reference" can only take place if the document referred to exists and is properly motivated. Nevertheless, this was not the case.

Court of Cassation, judgment of 15 June 2022

In this judgment, the Belgian Court of Cassation validates the decision of the Brussels Court of Appeal, after having referred a question to the Constitutional Court for a preliminary ruling on the rehabilitation and deletion of information related to a person's mental state.

Under Belgian law, rehabilitation allows the effects of a criminal conviction to be erased if certain conditions are met. This measure aims to reintegrate the convicted person into society. Following a rehabilitation decision, the mention of the conviction is removed from the criminal record. At the same time, another legal provision (art. 621 of the Criminal Procedure Code) prohibits the rehabilitation of a person who has been interned. In a decision already commented in the previous report, the Constitutional Court was asked by the Belgian Court of Cassation to an-

swer the question of whether this legal provision violates the principles of equality and non-discrimination, in particular because the continued registration of the internment decision in the criminal record reveals the past and the mental state of the person (i.e. an element of his or her private life). The Constitutional Court answered that internment is a measure whose nature and effects cannot be equated with those of a criminal conviction, and that it is justified that rehabilitation cannot be applied to an internment decision. The legal provision is therefore valid. Hence, the Court of Cassation refuses to overturn a judgment of the Brussels Court of Appeal (Indictment Division) which rejected the application for rehabilitation of a person who had been interned, on the grounds that the Belgian legal provision did not allow rehabilitation to be granted to an interned person. The Court of Cassation considered that the court had legally motivated its decision.

DATA PROCESSING OF DATA CONCERNING INDIVIDUAL OFFERING HOUSING SERVICES ON PLATFORMS

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 162/2022 of 16 November 2022

The BDPA ruled on GDPR compliance of surveys sent by the Tourist Office of Flanders (the defendant) to housing intermediaries in order to obtain personal data of housing operators to carry out controls.

The authority decided to investigate a practice of the defendant which consisted in sending request to Airbnb in order to obtain personal data of individuals offering housing services through the platform. The defendant however argued that the data processing was necessary to comply with a legal obligation (art.6.1.c. GDPR). In line with this argument, the litigation chamber noted that article 10 of the Flemish decree of 5 February 2016 on housing grants to the defendant's inspectors the duty to verify compliance with the requirements on touristic housing services. In addition, article 11 of this decree contains three different cases in which personal data can be requested, in a targeted manner, from housing intermediaries such as Airbnb. These cases include, among others, clearly delineated surveys. This was further confirmed in the preparatory works of the decree. Thus, the BDPA considered the data processing as necessary to apply the housing legislation and to comply with the defendant legal obligation. Regarding the data collected from intermediaries (e.g. address of the housing, name and email address of the housing operator), the BDPA also considered it as necessary for the processing. Therefore, the processing was lawful and did not violate data-minimisation principle. In contrast, the BDPA found violations of the transparency principle and the data subjects' rights of information (arts. 5, 12, 13 and 14 GDPR). In this sense, the privacy policy on the defendant's web portal contained outdated and incomplete information (e.g. the privacy policy contained references to the repealed law transposing the data-protection directive and only mentioned the possibility to lodge a complaint before a supervisory body established by a federated entity). Finally, the defendant failed to consult its DPO in due time regarding the processing (violation of arts. 38 and 39 GDPR). Consequently, the authority issued reprimands for these violations.

Constitutional Court, judgment 148/2022 of 17 November 2022

The Constitutional Court was asked to rule on the validity of an Order (i.e. a legislative norm adopted by a federated entity) obliging intermediaries to provide, to the tax administration, data on users offering housing services via their platforms.

Airbnb (the claimant) brought an action for annulment before the Constitutional Court against article 12 of an order of the Brussels-Capital Region of 23 December 2016 on the regional tax on touristic housing. This provision applies to intermediary housing-services providers such as the claimant. The first paragraph creates a duty to provide, on written demand, to the tax administration of the Region data relating to operators offering housing services in the Region through their platforms. If an intermediary fails to provide the data, a fine of 10.000€ can be imposed (second paragraph). According to the claimant, the provision creates, among others, an unjustified interference with the rights to privacy and data protection of the individuals using its platform to offer housing services in the Region. In the decision, the Court recalled that such provision indeed interferes with the right to privacy of the operators and that the Brussels legislator is bound by the guarantees of the GDPR. The Court however considered the interference as reasonably justified. To this extent, the provision aims to achieve legitimate objectives, which are the correct establishment of the regional tax on touristic housing and the verification of the operators' compliance with their tax duties. Fur-

thermore, the data to provide (i.e. name and address of the operator, contact details of the housing establishment, number of nights and establishments operated during the year) are sufficiently delimited. Finally, data transmission is not automatic and tax-administration's officials are bound by professional secrecy. Therefore, the Court upheld the first paragraph. In contrast, the Court decided that the impossibility to diminish the amount of the fine is contrary to the requirement of imposing proportioned punishments (violation of arts. 10, 11 of the Constitution and art.6 of the European convention on human rights). Hence, the Court annulled this paragraph.

RELATIONS BETWEEN INVESTIGATIVE POWERS OF THE TAX ADMINISTRATION AND THE RIGHTS TO PRIVACY AND DATA PROTECTION

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 134/2022 of 15 September 2022

The BDPA had to rule on a complaint filed against the tax administration (SPF Finances) for data-processing operation during tax investigation.

In this case, the defendant collected personal data while visiting various undertakings in which the claimant is involved. Then, the defendant sent to the same undertakings notifications of extension of the investigation which contained data on private trips of the claimant (e.g. locations and costs). According to the claimant, this practice resulted in violations of the GDPR. In its decision, the litigation chamber first recognised that it may sometimes be complicated for a claimant to identify the data controller. In such cases, the BDPA is competent to establish its identity. The authority also confirmed that the defendant determined purposes and means of the processing (by collecting data from undertakings and choosing which data to include in the notifications). Furthermore, the defendant is de jure qualified as data controller by the Belgian act of 3 August 2012 on data processing carried out by SPF Finances. Then, the litigation chamber recalled that data processing done on this basis falls within the scope of the BDPA's competences. In the same time the decision recalls that, in accordance with its "closing with no further action" policy, it is not the authority's priority to intervene in ongoing administrative proceedings. Although the authority is competent to verify the necessity of data processed for a tax investigation (i.e. the public interest task of the defendant) it must show extreme restraint. Therefore, it cannot substitute itself for the tax administration, which has a broad discretionary power to assess which data are necessary to carry out a proper tax investigation and to perform its tasks. Furthermore, tax proceedings – including data-protection issues – can still be subject to the appreciation of a judicial court. For this reason, the BPDA decided to reject the complaint.

Constitutional Court, judgment 162/2022 of 8 December 2022

The Constitutional Court refused to annul a law that imposes inclusion of additional personnel data in an already-existing database called "Point de Contact central" (PCC) managed by the National Bank of Belgium (NBB).

Before the Constitutional Court, two natural persons and a legal person (the claimants) requested the annulment of articles 18 to 22 of the program act of 20 December 2020. The contested provisions created a duty for financial entities (e.g. banks and credit institutions) to provide additional data related to taxpayers in the PCC. The data include the periodic balances of banks and payment accounts as well as the periodic aggregate amount of certain financial contracts. The provisions also allow the tax administration in charge with VAT to access the data where evidence of tax fraud exists (as it was already the case in the field of income taxation). The claimants alleged that such practices constituted an unjustified interference with the right to privacy. However, the Court rejecyed the complaint on several grounds. First, according to the Court, all the purposes aimed by the PCC database must be considered while assessing the validity of the contested provisions. To that extent, the mandatory inclusions of the additional data aims to fight tax evasion but also helps judicial authorities and intelligence services to contrast terrorism and serious crime. Second, subject to a prior opinion of the BDPA, any person entitled to receive data from the PCC must be explicitly authorised by the legislator to request them in order to perform a task in the public interest enshrined by law. Third, in the field of taxation, the data can only be requested where there is evidence of tax evasion. Fourth, citizens can request to the NBB the identity of any person who has received his or her data in the six months prior to the request. Finally, the Court also notices that the persons entitled to receive the data must ensure confidentiality and cannot process data for unlawful purposes.

Constitutional Court, judgment 103/2022 of 15 September 2022

An action for annulment is brought before the Constitutional Court against the Belgian act of 20 December 2019 transposing the EU directive 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements (Directive 2018/22).

In this case, claimants - including the national bar associations and the institute of chartered accountants - requested the annulment of the contested act transposing the EU directive 2018/822. This act modifies several Belgian tax codes (i.e. income tax code, code of registration and mortgage fees, inheritance tax code and code of miscellaneous duties and taxes). In substance it creates a duty to provide the tax administration with data relating to cross-border arrangements that indicate the risk of tax avoidance. Information on these arrangements is then automatically shared with other member states. Such duty applied to intermediaries (i.e. any person which, among others, designs or markets reportable arrangement, or offers advices in this regard). Where intermediaries are subject to professional secrecy, the duty of declaration applies to other intermediaries and ultimately to the taxpayer. For marketable arrangements (i.e. arrangement that can be implemented without substantial customisation) intermediaries must also provide, every three months, a report containing updates such as name of the concerned taxpayers. In such case, they cannot invoke professional secrecy. Therefore, the claimants argued, among many claims, that this mechanism infringes upon attorney-client privilege as well as the duty of confidentiality applying to other professions. Regarding this claim, the Court recalled that attorney-client privilege is an essential component of the rights to a fair trial and privacy, which also apply to legal advice provided outside legal proceedings. The Court acknowledged however that privilege does not extend to information otherwise disclosed, such as the ones provided in periodic reporting. Hence, the Court considered that the absolute privilege is not proportionate since lawyers can still provide information to be declared to the taxpayer (especially as marketable arrangements do not need substantial customisation). Likewise, absolute priviledge for other professions is also not proportionate. Thus, the Court annulled the provisions of the codes as modified. Among others, the claimants also argued that the mechanism of mandatory declaration was contrary to rights to privacy and data protection. Regarding this claim, the decision highlights that a duty to disclose also lawful, genuine and not abusive arrangements is created by the Directive. Therefore, the Court referred a question to the EU Court of Justice for a preliminary ruling. In particular, it questions whether the reporting obligation created by the Directive does not constitute a disproportionate interference with the rights to privacy and data protection.

PERSONAL DATA PROCESSED FOR EVIDENTIAL PURPOSES

Corporate Court of Namur (2nd chamber), order of 26 July 2022 available in Revue de jurisprudence de Liège, Mons et Bruxelles (J.L.M.B.), 2023, no 1, p.7

The Court considers that consulting and copying an agenda, in order to use it as evidence to support a legal claim, is a processing of personal data within the meaning of the GDPR.

Under Belgian law, in civil disputes, the use of unlawfully-obtained evidences cannot be dismissed. This principle applies unless (1) the law provides otherwise, (2) the obtaining of the evidence would undermine its reliability or (3) the obtaining of the evidence compromises the right to a fair trial. In the case at hand, the Court had to rule on a dispute concerning an alleged breach of a non-competition clause in a business-transfer agreement. In order to prove the breach of the clause the claimant consulted the defendant's agenda. On this occasion, he discovered, the presence of suspicious appointments and events. According to the Court, the consultation and making a copy of a diary must be considered as "processing" within the meaning of the GDPR. In order to ensure compliance with the GDPR, the Court considers that in the case of personal data collected in the context of the preparation of a file to support a legal claim (i.e. data processed for evidentiary purposes) it is necessary to verify, (1) whether the data have been processed fairly and lawfully, (2) whether the purposes are specified, explicit and legitimate and (3) whether the data are relevant, adequate and strictly necessary. According to the Court, the consultation of the agenda for a period not covered by the non-competition clause does not constitute the pursuit of a legitimate interest on the part of the applicant. Hence, the data were not processed in accordance with article 5 of the GDPR. However, as the copy of the consulted

agenda was disclosed to the other party, the rights of defence were respected and there was no breach of the right to a fair trial. The Court also considers that the evidence of contacts with customers (which is supported by the agenda) is a useful and necessary element for the resolution of the dispute. Therefore, the Court does not reject the document and declares it admissible evidence.

PERSONAL DATA PROCESSED IN THE FIELD OF EDUCATION

Belgian Data Protection Authority (BDPA) (Litigation chamber), decision 175/2022 of 28 November 2022

The BDPA had to rule on complaints filed against an educational institute for social promotion (the first defendant) and its education authority (the second defendant).

The BDPA received two complaints filed by a former student of the first defendant against the first defendant (not possessing the legal personality) and the second defendant (having the legal personality). The first complaint was directed against the sending of a group email to several students with the email addresses of all recipients visible. The second concerned the public display of students' results with the mention of their names and date of birth. The BDPA determined the capacity of each of the defendants in order to determine who was accountable for the processing. To that extent, the litigation chamber recalled that an entity such as the first defendant which has no legal personality (e.g. a de facto association) can be qualified as data controller. Considering the factual elements of the case, the second defendant was however the data controller. Therefore, the authority decided to close the complaint against the first defendant. With regard to the two complaints, the BDPA analysed whether the sending of the email to all students was based on a specific purpose and was relying on a lawfulness ground (articles 5.1.a. and 6 RGPD). In the present case, given the description of the limited purposes for which the email address was collected at registration, the further processing (i.e. to allow communication in the framework of a course) cannot be qualified as permissible. Nor did the defendant rely on a permissible lawfulness basis for the processing at issue. It also considers that the principles of transparency and minimisation have not been respected. In particular, the decision highlights that public display of students' results with name and date of birth instead of results and matricula infringes the GDPR. The BDPA concluded that Articles 5.1.a., 6 and 12.1. GDPR were violated. It therefore issued reprimands.

FRANCE

edited by
Mehdi KIMRI, Ph.D. Candidate in Public Law, University of Côte-d'Azur
Julien MONGROLE, Ph.D. Candidate in Public Law, University of Limoges
Raphaël MOURERE, Ph.D. Candidate in Private Law, University of Côte-d'Azur
Quentin RICORDEL, Ph.D. Candidate in Public Law, University of Limoges
Guillaume TOURRES, Ph.D. Candidate in Public Law, University Paris 1 Panthéon Sorbonne

DIGITIZATION OF ADMINISTRATIVE PROCEDURES

Investigation by the Defender of Rights, 26 January 2022, on the availability of public service telephone platforms

On 26 January 2023, the Defender of Rights and the National Consumer Institute published the results of a joint survey on the availability and quality of the telephone platforms of four public services.

In France, the dematerialization process initiated by the Government through the "Public Action 2022" Plan is the subject of significant debate, particularly as regards the effectiveness of access to people's rights. The massive use of tele-services and the concomitant closure of reception areas to the public deprive people who do not have adequate computer equipment or knowledge of regular access to public services. The impossibility of accessing public services online leads to situations of non-use of rights and aggravates the financial or social precariousness of certain users. Several reports by the Defender of Rights have reported on these issues, as is the case with the 2019 report "Dematerialization and inequalities of access to public services" (www.defenseurdesdroits.fr/fr/rapports /2019/01 /dematerialisation-et-inegalites-dacces-aux-services-publics), supplemented in 2022 by a second report "Dematerialization of public services: three years later where are we? (www.defenseurdesdroits.fr/fr/rapports/2022/02/ rapport-dematerialisation-des-services-publics-trois-ans-apres-ou-en-est-on).

Faced with the gradual closure of public-

service counters, the use of administrative telephone platforms is essential in order to maintain several methods of access to public service. With a view to testing the accessibility of public services by telephone, the Defender of Rights and the National Consumer Institute conducted a survey on the availability and quality of public-service telephone platforms. This survey follows a first study published in 2016 “Telephone reception and dematerialization of public services. The results of a mystery investigation”.

This new study focused on the telephone platforms of four French public services. Namely: the Family Allowance Fund (CAF), Pôle Emploi, the Health Insurance and Pension Insurance (CARSAT). It aimed to determine “whether it was easy to reach these organizations by telephone and to collect useful information to benefit from a benefit”. To do this, several “caller profiles” were used to contact the administrations concerned and obtain information. Among these profiles, it is possible to mention: a person with internet access, a person who does not have internet access, a person who does not have a good command of French language, and finally an elderly person with internet access.

The conclusions of this investigation are divided. If the “friendliness” of the interlocutors has been noticed, the rate of satisfactory answers never exceeds 60% and the waiting time before obtaining an interlocutor is generally more than 9 minutes. In other words, “on the 1,500 calls made as part of the survey, 40% were unsuccessful”. In addition, the Defender of Rights denounces the systematic referrals to the teleservices of the administrations concerned, despite the presence among the profile of callers of a "person without internet". A questionable practice more generally, since according to the National Institute of Statistics and Economic Studies (INSEE), nearly 17% of the French population suffer from illiteracy, and 7% do not have internet access at home.

Decree no 2023-64 of 3 February 2023 creating a processing of personal data called "NATALI"

The decree of 3 February 2023 aims to create a processing of personal data called NATALI. This teleservice is set up to allow users to carry out electronically the steps necessary to obtain French citizenship, to francize surnames and first names and to authorize the loss of French citizenship.

Since the beginning of 2021, the procedures relating to the applications and renewals of residence permits have been increasingly dematerialized. Several regulatory texts have intervened in this direction, this is particularly the case of decree n ° 2021-313 of 24 March 2021, the order of 27 April 2021 and the order of 19 May 2021. These various texts, which aimed to generalize the use of a teleservice for applications for certain residence permits were challenged before the Council of State, which ruled on the occasion of a judgment of 3 June 2022 no. 452798. The administrative judges considered that the obligation imposed on users to use a teleservice is not illegal, but that it must be accompanied by additional measures so as not to exclude people experiencing some difficulty with the digital tool.

It is clear that despite these decisions, the Government's objectives are tending towards an increasing generalization of teleservices in the context of applications for residence permits. The decree of 3 February 2023 authorizes the Minister of the Interior to implement the processing of personal data "NATALI". These teleservices have several purposes (article 1):

First, to allow foreigners to complete the procedures for acquiring nationality online by reason of marriage, ascendant status or status of brother or sister of French nationality. The procedures for acquiring French nationality by decision of the public authority and for reintegration into nationality are also covered; francization of surnames and first names; and authorization to lose the French nationality.

Secondly, to allow the central and local services of the ministry, as well as the diplomatic and consular authorities to ensure the processing of requests, but also that of administrative and contentious appeals that may occur.

Third, to allow users or their representative to exercise administrative recourse against decisions concerning them.

The personal data processed in the "NATALI" automated processing (article 2) are mentioned in the first appendix to the decree, and are only accessible within the "limit of the need to know" by strictly identified agents, individually designated and specially authorized (Article 3). These include agents responsible for applying the regulations relating to the acquisition, withdrawal, forfeiture and loss of French citizenship and coming under the central services of the Ministry of the Interior. and the Ministry of Foreign Affairs, also agents of the prefectures and sub-prefectures and agents of the diplomatic or consular services. With regard to the recipients of these personal data, this decree establishes a list in its article 4, distinguishing them ac-

cording to the type of data concerned.

The retention periods for personal data are mentioned in article 5. For data corresponding to the identifier, the password, as well as those resulting from communications between the administration and the person concerned, identified benefiting from a user space and those concerning the identifier of the agent, the legal representative, the lawyer or the spouse, the retention period is 3 years from the final decision of the administration. For all other data mentioned in the appendix, the retention period is 3 years from the date of publication in the Official Journal of the decree of naturalization, reintegration into French nationality or release from ties of allegiance, or from the date of registration of the declaration or francization decree. Article 5 provides for variable retention periods in the event of refusal and a decision to classify without further action.

Finally, Articles 6 and 7 provide the procedures for exercising the rights relating to the protection of personal data.

PROTECTION OF PERSONAL DATA

Commission nationale de l'informatique et des libertés (CNIL), Deliberation 2022-118 of 8 December 2022

The CNIL had the opportunity to rule on 8 December 2022 on the bill relating to the 2024 Olympic and Paralympic Games, presented by the Government to the Council of Ministers on 22 December 2022.

The bill relating to the 2024 Olympic and Paralympic Games provides for several derogations from ordinary law in order to ensure the proper organization of the event. Several provisions of the bill present strong stakes in terms of personal-data protection. This is particularly the case:

- Authorizing the examination of the genetic characteristics or the comparison of the athlete's genetic fingerprints for the purposes of the fight against doping (article 4);
- Compliance of the Internal Security Code (CSI) with the GDPR and the law of January 6, 1978 (article 5);
- The use of augmented cameras (article 6);
- The extension of the video-protection images that the agents of the internal services of the SNCF and the RATP can view when they are assigned within the information and command rooms coming under the State (article 7);
- The extension of the screening procedure provided for in article L211-11-1 of the CSI to fan-zones and participants in major events (article 9);
- The possibility of setting up body scanners at the entrance to sports arenas (article 10).

It is on all of these articles that the CNIL had to rule in the context of the deliberation of 8 December 2022. Particular attention will be paid to articles 4,5,6,7 and 10 of the bill.

Firstly, concerning the examination of genetic characteristics in the context of anti-doping tests. Article 4 of the bill aims to ensure compliance with domestic law with the provisions of the World Anti-Doping Code. To do this, the article provides for several derogations from the provisions of the Civil Code for the purposes contrasting doping. The CNIL, while acknowledging the need to adapt domestic laws, stresses that "these would be particularly intrusive tests, which significantly derogate from the principles currently governing the analysis of genetics in the Civil Code". In addition, the regulator urges the Government to explain the conditions for informing and obtaining the consent of the athlete subject to these analyses.

Secondly, on bringing the Internal Security Code (CSI) into compliance with the General Data Protection Regulation and the Data Protection Act of 6 January 1978. Indeed, the bill intends to bring the CSI, particularly Articles L.251-1 and L.255-1, within the provisions of the GDPR and the French Data-Protection Law regarding the protection of personal data. While acknowledging the benefit of bringing the video protection regime provided for by the CSI into compliance, the CNIL denounces "the choice to modify the existing provisions as a minimum [...]" and calls for a "more global" reform of the regime relating to the "processing of images in spaces open to the public […]" as well as "general" compliance with the CSI.

Third, on the experimentation of "augmented" cameras. Article 6 of the bill aims to experiment with "algorithmic processing of automated analysis of images from video-protection devices and cameras installed on aircraft in order to detect and report events in real time.". These systems based on artificial-intelligence systems are intended to "ensure the security of sporting, recreational or cultural events which, by their size or their circumstances, are particularly exposed to the risk of acts of terrorism or risk of serious harm to the safety of persons". As such, any use of augmented cameras for other purposes is ruled out. The regulator recognizes the legitimacy of these objectives, but recalls "that the de-

ployment, even experimental, of these devices of augmented cameras is a turning point which will contribute to defining the role which will be entrusted in our society to these technologies, and more generally to "artificial intelligence". In addition, it specifies that the guarantees provided for by the bill are consistent with the recommendations formulated in its position paper on the deployment of augmented cameras in public spaces, published in July 2022 (www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position). To know:

- "An experimental deployment;
- Limited in time and space;
- For certain specific purposes and corresponding to serious risks for people;
- The absence of biometric data processing;
- The lack of reconciliation with other files;
- The absence of automatic decision-making: the algorithms are only used to signal potentially problematic situations to people who then carry out a human analysis".

Fourthly, with regard to the extension of the video surveillance images that the agents of the internal services of the SNCF and the RATP can view. Article 7 of the bill aims to extend the spectrum of video-protection images that can be viewed by agents of the internal security services of SNCF and RATP, the two main transport players in the Ile-de-France region. This extension aims to ensure "better management of the flow of supporters going to sites served by the means of transport of the two operators, or leaving them at the end of the sporting event" and to allow "the improvement of the communication between the different people involved in the flow of people in the context of major sporting events". For the CNIL, the possibility offered to SNCF and RATP agents to access more images should not lead to an extension of their competence at the same time. These remain limited to missions of prevention and safety of persons and property. Furthermore, the CNIL suggests that the bill be clarified so as not to imply that access to the images can be done without restriction.

Lately, on the possibility of setting up body scanners at the entrance to sports arenas. The implementation of body scanners proposed by article 10 aims to streamline and secure people's access to areas determined by decree. For the CNIL, the various conditions defined by the bill (consent of the data subject, respect for anonymity, system blurring the visualization of the face, prohibition of the recording and storage of images, etc.) makes it possible to reduce violations "to the privacy and intimacy of the persons concerned". On the other hand, it recalls that these devices constitute processing of personal data within the meaning of the Communication from the Commission to the European Parliament and the Council on the use of security scanners at airports in the European Union of 15 June 2010 (COM/2010/0311 final) and that they remain subject to the relevant regulations. In addition, the CNIL calls for particular vigilance with regard to the procedures for obtaining consent and informing the persons concerned.

Court of Cassation, 1st Civil Chamber, 5 January 2023, No. 22-40.017

In a decision dated 5 January 2023, the Court of Cassation refused to transmit the priority question of constitutionality raised in the context of a dispute with the Autorité de Régulation de la Communication Audiovisuelle et Numérique (French regulatory authority for audiovisual and digital communication), concerning measures to block access to pornographic sites in order to protect young people.

In this case, a number of internet service providers were challenged in relation to access by minors to websites containing pornographic content. This access is open to any user who simply declares that he or she is not a minor. However, article 227-24 of the Penal Code punishes the offence of manufacturing, distributing or trading a pornographic message when this message is likely to be seen or perceived by a minor. Moreover, the third paragraph of the article specifies that the offence is constituted "even if the access of a minor to the messages [...] results from a simple declaration by the minor indicating that he or she is at least eighteen years of age".

The Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) is the independent administrative authority empowered to control the existence of such access to pornographic content. On the basis of article 23 of the law of 30 July 2020 no 2020-936 aiming at protecting victims of domestic violence, the president of ARCOM has the power to give formal notice to any person whose activity is to publish a service of communication to the public on line, so that the latter takes all the necessary measures to prevent the access of minors to pornographic content. In case of non-fulfilment of the injunction, the president can then refer the matter to the judicial court in order to close access to the content according to the accelerated procedure on the merits; which in this case has

been done. At this stage of the proceedings, one of the companies involved in the case raised a priority question of constitutionality concerning the provisions of article 23 of law no 2020-936.

Although the provision in question defines, at first glance, the criminal offence as well as the conduct that may give rise to a sanction in sufficiently-clear and precise terms, the character of necessity, adaptation and proportionality to the objective of protecting minors could raise questions. Indeed, by deeming insufficient a control by declaration, article 23 of the law no 2020-936 imposes on internet-access providers as well as on publishers of pornographic content sites, and more generally of content unsuitable for minors, to implement a stricter control. What about the modalities of such a stricter control, which presents practical and economic difficulties? The Paris Court of Justice has thus transmitted the priority question of constitutionality to the Court of Cassation, which has examined it. Therefore, article 23-4 of the organic law no 2009-1523 of December 10, 2009 on the application of article 61-1 of the French Constitution provides the conditions for the examination of a priority question of constitutionality by the French Constitutional Council. The questioned provision must be at issue in the pending litigation, it must not have already been declared in conformity with the French Constitution by the Constitutional Council and, finally, the question must be new or present a serious character. The Court of Cassation noted that if the first two conditions were met, the question was not new in that the provision had already been applied by the Constitutional Council. In addition, the court noted that "the infringement of the freedom of expression, by requiring the use of a device to verify the age of the person accessing pornographic content, other than a simple declaration, is necessary, appropriate and proportionate to the objective of protecting minors. The measures to control the age of users will thus have to be reinforced, requiring operators to bear the cost and responsibility of a new processing in the sense of personal-data protection law.

SUMMARY INJUNCTION AND PROSECUTION DISTINCTION

Paris judicial court, summary order 21 December 2022, Noctis Event et M. X. / Wikimedia Foundation Inc

In a summary order dated 21 December 2022, issued on the basis of article 145 of the French Code of Civil Procedure, the Paris judicial court distinguished between a judicial-information measure and a protective measure ordered in summary proceedings. The court held that the communication of identification data of a user who created a Wikipedia page under the cover of a pseudonym constitutes an investigative measure legally admissible by the judicial judge, independently of the principle according to which only the public prosecutor has the right to prosecute.

In this case, the company Noctis Event and its director were targeted in a Wikipedia page created by an unknown person acting under a pseudonym. The elements gathered in the page showed the particular malice of the author against the designated company and its manager: "he cheats at his baccalaureate, with earphones and a cheat sheet", "he is a cousin of the anti-Semitic director Pierre Ramelot", "he is a cousin of the pedophile writer Henry de Montherlant". The company and its director then asked the Wikimedia company to communicate the identification data of the author of the litigious page. Let us recall that article L.34-1 of the Code of the posts and electronic communications stipulates that the operators of electronic communications are held to preserve, for the needs "in particular of the penal procedures" - but not only, the information relating to the civil identity of the user until the expiration of a 5-year deadline as from the end of validity of its contract, and the other information provided by the user at the time of the creation of an account, until the expiration of a one-year deadline as from the closing of the account. However, Wikimedia refused to make the disclosure despite being ordered to do so by a motion order. Wikimedia was consequently summoned in summary proceedings by the company Noctis Event to comply.

On the basis of article 145 of the French Code of Civil Procedure, the court examined the "legitimate reason" put forward by the plaintiff company. The existence of this legitimate reason is a prerequisite for any investigative measure aimed at preserving or establishing, before any trial, evidence of facts on which the solution of a dispute could depend. Exercising its discretion as a judge of the merits, the court concluded that the filing of a lawsuit for denigration or on the basis of the criminal offence of cyberstalking did constitute a legitimate reason. The court notes that the exercise of such an action is not obviously doomed to failure in this case; the identification of the author of the page being however essential to its success. Thus, the court judged that the communication of the identification data

was necessary for the exercise of the right to evidence and proportionate to the antinomic interests at issue.

The judgment has the advantage of distinguishing between the taking of a precautionary measure ordered by the judge and an investigative measure taken in the context of a judicial investigation, which is conditional on the exercise of the public prosecutor's action. Article 80 of the French Code of Criminal Procedure stipulates that a judicial investigation can only be opened upon the request of the public prosecutor. The judicial investigation must make it possible to determine the existence of an offence and to identify the perpetrators. However, the Paris judicial court specifies that "the mere fact that the public prosecutor has the opportunity to prosecute, as the Wikimedia Foundation Inc. maintains, cannot suffice to render the requested investigative measure, which is aimed at identifying the author of these acts, unlawful. The judge can thus order communication measures relating to facts likely to be subject to criminal sanctions before the public prosecution is initiated, insofar as the evidence concerned is necessary for the exercise of a civil liability action; in this case for denigration. Indeed, the interest of this evidence cannot be limited to the framework of the investigation carried out during a judicial investigation in anticipation of a criminal trial.

COUNTERFEITING AND RESPONSE TO A PUBLIC INVITATION TO TENDER

Court of Cassation, 1st Civil Chamber, 5 October 2022, No. 21-15.386, Entr'ouvert / Orange and Orange Business Services

In a decision dated 5 October 2022, the First Civil Chamber of the Court of Cassation clarifies that the owner of a copyright on a software that he has licensed is entitled to bring an action for infringement against the licensee who has used said software to respond to a public tender, in violation of the stipulations of the license agreement.

In this case, the company Entr'Ouvert conceived a software named “Lasso” allowing the installation of a unique authentication system. It diffused this software under free license. In order to answer the call for tender of the French State for the realization of the portal "My public service", the company Orange had developed a software platform for management of identities and means of interface for service providers. But this platform integrated the Lasso software. The company Entr'Ouvert then sued the company Orange for copyright infringement and economic parasitism, arguing that this use of its software was not in conformity with the stipulations of the free-license contract. In a decision dated March 19, 2021, the Paris Court of Appeal awarded Entr'Ouvert the sum of 150,000 euros in damages for economic parasitism exercised by the company Orange. The sum was far from the 500 000 euros of damages initially requested by the company, for lack of sufficient evidence of the extent of the economic damage suffered, according to the assessment of the judges of the court. In addition, the judges of appeal declared the copyright-infringement action of the company Entr'ouvert inadmissible. Entr'ouvert then appealed against this decision.

Pursuant to Article L. 335-3, paragraph 2, of the French Intellectual Property Code, Articles 7 and 13 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, and Article 1 of Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, the Court of Cassation found that in the case of copyright-infringement on software, the owner does not benefit from the guarantees provided for in Articles 7 and 13 of Directive 2004/48/EC of the European Parliament and of the Council of April 29, 2004, when he acts on the basis of contractual liability under ordinary law. Consequently, the judges of cassation specify that the owner can act in infringement. Their reasoning takes into account the interpretation of the judges of the Court of Justice of the European Union of the aforementioned European directives.

The judges of the Union had indeed specified in a judgment of December 18, 2019, C-666/18, that "the infringement of a clause in a computer-program licensing agreement, relating to the intellectual property rights of the holder of the copyright in that program, falls within the scope of infringement of intellectual property rights, within the meaning of Directive 2004/48, and that, consequently, that holder must be able to benefit from the safeguards provided for in that directive, irrespective of the system of liability applicable under national law. However, in this case, the judges of appeal did not take into account elements other than economic factors, such as the moral prejudice caused to the right holder by the infringement. Furthermore, the compensation awarded to Entr'Ouvert did not include, as an alternative, a lump sum of damages, based on elements such as, at least, the amount

of the royalties or fees that would have been due if the infringer had requested permission to use the intellectual-property in question. The company Entr'Ouvert could not indeed profit from the guarantees offered by directive 2004/48 within the framework of an action in contractual civil liability. In this action for non-performance of the contract of license, the amount of the damages cannot exceed what is foreseeable at the conclusion of the contract or what the parts envisaged conventionally; according to former article 1147 of the French Civil code in its version applicable to the case (current article 1231-1 of the French Civil code). The re-exploitation in the response to a public contract in contravention of the stipulations of a software-license agreement, is thus likely to expose the candidate to the payment of damages for copyright infringement.

ITALY

edited by
Alessia PALLADINO, Ph.D. in Administrative Law, University of Naples Suor Orsola Benincasa

EXCLUSION OF THE ECONOMIC OPERATOR IN CASE OF NEGLIGENCE IN E -PROCUREMEN PROCEDURES

Regional Administrative Court of Umbria, decision 761/2022 of 27 October 2022.

In this ruling the Regional Administrative Court of Umbria rules that the competitor who tried to upload the tender documents on the Me.pa telematic platform within the fixed time, but could not finalize the sending and does not take a diligent actions by immediately reporting the malfunctioning and asking for remedies, shall be excluded from such tender procedure.

The Regional Administrative Court of Umbria, Perugia, clarifies the specific duties of fairness, accountability and diligence upon to the economic competitor who decides to join a public tender and tries to upload the tender documents on the telematic platform.

The dispute arose from the action brought before the Regional Administrative Court of Umbria, by an economic operator who contested the exclusion from a simplified-negotiated procedure on the Me.pa platform.

Due to a technical malfunctioning, the operator alleged the impossibility of entering the fields reserved for the technical and economic documentation.

Consequently, they decided to upload the technical and economic offer in the field relating to the administrative documentation. Therefore, to ensure the respect of secrecy and impartiality, the offers were distinguished in three different files.

In its judgment of 27 October 2022 no 761, the Regional Administrative Court of Umbria rules that whenever the tender procedure is characterised by a clear separation between the evaluation phase of the technical tender and the evaluation phase of the economic offer, the principle of unfairness means that until the evaluation of the technical elements is completed, the economic offer must be kept secret, to avoid any possible influence on the evaluation of the technical elements. In particular, the mere possibility of knowing the extent of the economic offer, before the technical one, is prone to jeopardize the guarantee of impartiality of the assessment.

Therefore, the Court recalls long –-lasting opinions and previous judgments (Regional Administrative Court of Lazio, Rome, sect. II, decision of 16 December 2021, no 13081), which underline a renewed-accountability attitude addressed to the economic operator.

The Court argues that widespread e-procurement calls for particular care and diligence in uploading the documents, with the consequent impossibility of attributing to the Contracting Authority any type of anomaly in the mechanism of re-registration.

Beside all, in case of proven technical malfunctioning of the platform, which avoids the transmission of the tender documents, the economic operator must take diligent steps by immediately reporting it to the Contracting Authority, and asking for remedies provided by Article 79, paragraph 5-bis, of the legislative decree no 50/2016.

In this regard, the operator must be diligent, by asking for (i) an extension or (ii) a suspension of the deadline, as well as (iii) the opening a ticket for technical support. On the contrary, the Court underlines that in the case at issue the economic operator just uploaded the tender documents together, providing a mere screenshot, that it found unsuitable to prove the platform malfunction.

As a consequence, the Court states that the exclusion was legitimate.

The analysis of the judgment of the Italian Regional Court of Umbria allows to conclude that, in the event of a software malfunctioning, the economic operators which have started uploading the documents and discover the failure,

shall act diligently by immediately reporting the malfunctioning to the contracting authority, and asking for remedies to complete their submission within a reasonable time.

In this regard, the decision of the Administrative Regional Court of Umbria confirms the legal precedents, which suggest a renewed morphology of economic operator's duties in the e–procurement sector.

PROOF OF PUBLICATION ON A WEBSITE THROUGH ITS CACHE

Council of State, Section V, decision no 8123/2022 of 21 September 2022.

The Council of State rules that the allegation of the Google cache, referred to the Contracting Authority institutional website, is eligible to prove the publication of the contracting award notice, as well as to provide the date of its publication.

The decision of the Council of State provides an innovative overview towards the usage of technology to prove the publication dynamics occurred in the Contracting-Authority institutional website.

In particular, it offers the chance to reflect upon the scope of the Google cache.

The appeal arose from the dispute, decided by the Regional Administrative Court of Naples with the decision of the 31 August 2021, no 5660.

The appellant, ranked second at the end of the tender, with a total score of 69.09 points (having obtained 66.38 points for the technical tender and 2.71 for the economic tender, corresponding to a 4.25% discount), against the winner who scored 79,17 points (in details, 69,17 points for the technical offer and 10 for the economic offer, with a decrease of 58%), has appealed all the acts of the tender, as well as the contracting-award notice.

Thus, at a first glance, the defendant claims for the inadmissibility of the action, arguing that it has been proposed late, out of the legal terms: in details, they state that the contracting-award notice was published on 19th January 2021, whereas the company notified the application more than three months later, on 21st April 2021 and filed it on 5th May 2021.

The Council of State preliminarily rejects the exception of inadmissibility for the lateness, proposed by the defendant.

In this regard, the Council underlines that the appellant company, while contesting that the tender-award notice was published on 19th January 2021, has proven that this notice actually appeared on the web no earlier than 2nd May 2021.

This statement has been confirmed by evidence of the cache registered from the portal www.google.it.

As a matter of fact, caching constitutes a process that allows to temporarily store copies of files, images, as well as web pages, to reduce loading time when a user visits a website.

Thus, the Contracting Authority's website page archived by the Google cache has revealed that the last publication on that website occurred on May 2nd 2021, at 6.53 am.

On this ground, the Council considers the appeal admissible.

PORTUGAL

edited by

Luís MANUEL PICA, Ph.D. in Public Law at the University of Minho (Portugal), invited Assistant Professor at the Polytechnic Institute of Beja (Portugal) and researcher at JusGov- Research Centre for Justice and Governance at University of Minho (Portugal).

Mário FILIPE BORRALHO, Master's student at Law School - University of Lisbon (Portugal), Solicitor, Teaching assistant at the Polytechnic Institute of Beja (Portugal)

THE PROTECTION OF PERSONAL DATA IN THE PUBLIC ADMINISTRATION

Deliberation no 1040/2022, of 2 November 2022 of the National Commission for Data Protection of Portugal (Comissão Nacional de Proteção de Dados de Portugal)

The national body responsible for protecting personal data has decided to condemn a public-administration body for failure to comply with the General Data Protection Regulation.

The National Commission for Data Protection (CNPD), as the Portuguese administrative agency responsible for supervising and enforcing compliance with the provisions relating to the protection of personal data, decided in deliberation nº. 1040/2022, of 2 November 2022, to impose a fine of EUR 170,000.00 on the municipality of Setúbal for breach of i) the principle of confidentiality (art. 5, paragraph 1(f) of the General Data Protection Regulation), ii) the principle of limitation of the right to access and rectifica-

tion of personal data (Article 5, paragraph 1(f) of the General Data Protection Regulation), of (iv) the principle of storage limitation (Article 5, paragraph 1(e) of the General Data Protection Regulation), and of (iv) the principle of transparency (Article 12 of the General Data Protection Regulation) and of the obligation to appoint a data-protection officer (Article 37 of the General Data Protection Regulation), particularly about the processing of personal data of Ukrainian refugees.

In the context of a procedure to support Ukrainian refugees creating a municipal-support line for refugees and the subsequent creation of a personal database of the same, it was decided that the personal data of the beneficiaries would be collected, without providing the necessary and mandatory information at the time of collection, as well as the context in which the collection was carried out, the duration or a reasonable period of time for its storage, and this database would be accessible by third parties without any protection mechanisms that sought to protect personal data. On the other hand, it was verified that there was no mandatory designation of a Data Protection Officer, being Setúbal City Council a municipal body, it was legally obliged to designate a person responsible for the protection of personal data.

In these terms, Setúbal Municipality was condemned of four offences of a misdemeanor nature.

THE PRACTICE OF PROCEDURAL ACTS IN THE ADMINISTRATIVE COURTS AND THE MANDATORY USE OF ELECTRONIC FORMAT

Judgment of the Central Administrative Court of the South of 6 October 2022

The administrative court decided that since the administrative process is exclusively electronic, the information contained in the forms must be duly filled out to avoid discrepancies with the attached files, otherwise only the content of the initial form will be considered.

According to the provisions of article 24 of the Procedural Code of the Administrative Courts, the proceedings before the administrative courts are electronic, and the procedural acts submitted in writing by the parties shall be presented in court by electronic means, by the respective representatives in the computer system of support to the activity of the administrative and fiscal courts (called SITAF), under the terms defined in Ministerial Order nº. 380/2017, of 19 December;

The practice of procedural acts is carried out by filling out the forms made available in the SITAF to which are attached, namely, files with the material content of the procedural document.

Where the forms contain fields for specific information, they should be filled in accordingly, even if such information is included in the attached file. Where there is a discrepancy between the information contained in the form and the file attached to it, submitted, and which is not corrected at the request of the interested party, in the general terms, or raised automatically, the information in the former shall prevail, even if the respective fields are not filled in.

Detecting the discrepancy in the information regarding the witnesses, the registry in compliance with the provisions of the reproduced paragraph 4 of Article 6 of Ordinance Nº. 380/2017, should notify the applicant to proceed, within 10 days, with the completion of the respective form made available in the computer system of support to the activity of administrative and tax courts, under penalty of considering only the content of the initial form.

Determination that has implicit the existence of two forms: the initial one not filled in or wrongly filled in the field concerning the witnesses, given the content of the evidentiary request in the attached defense - which were submitted in the SITAF and, therefore, are unsusceptible, in themselves, of edition or alteration -; and the one to be filled in, following notification to this effect, to put an end to the divergence of information on this matter - consisting of a request form which will follow a similar process to that used for registering the initial petition or the defense, allowing the representative to insert/add or edit, by substitution, parties, such as witnesses, registered (or not) in the SITAF in previous forms and attached files.

DUTY OF CONFIDENTIALITY ON DATA CONTAINED IN PROPERTY TAX RECORDS.

Ruling of the Supreme Administrative Court, 9 November 2022, Case no 0718/22.7BELRA

In this judgement, the Portuguese Supreme Administrative Court considered that information such as the tax-identification number and tax domicile of the owner of a certain building, contained in the property-tax records, constitute data subject to tax secrecy, and therefore can only be disclosed in the strict circumstances foreseen in Article 64 of the General Tax Law.

The property-tax records, kept by the tax au-

thorities (Tax and Customs Authority) for the purpose of taxation of real-estate assets, contain, namely, the characterization of the properties, the location and their taxable value, as well as the identity of the owners. This means those services receive daily requests for information (on the identity and address of the owner(s) of certain properties) from third parties (potential purchasers, owners of adjoining properties, lawyers, solicitors, etc.), with the disclosure of such data being refused on the grounds that they relate to and reveal the tax situation of the taxpayers.

In the case at issue, the court considered that tax secrecy may be defined as a data-protection regime, which covers not only the privacy of tax data themselves (those that express the taxpayer's tax situation - e.g., data relating to the valuation of the property or to tax exemptions), but also the taxpayers' personal data (data of a personal nature obtained in the exercise of or because of tax functions, that is, in the context of tax procedures or actions - such as addresses and tax-identification numbers). It also established that, although property-tax records fall within the concept of "administrative document", and a right of free access applies to these documents (article 5 of the Access to Administrative Documents Act - Law no. 26/2016, of 22 August), since they contain personal data, this right cannot prevail over the protection constitutionally-granted to the privacy of private life, so it will be necessary to invoke a direct, personal, legitimate and constitutionally protected interest that is sufficiently-relevant interest, justifying access to the information (being that the claim that there is a need to contact the owner of the land, or to know if they belongs to the public domain does not fulfill such requirements). Tax secrecy is maintained even if such data are or not freely accessible through other legal and institutional channels (e.g. land registry).

ACCESS TO ADMINISTRATIVE DOCUMENTS CONTAINING COMMERCIAL, INDUSTRIAL OR COMPANY SECRETS

Ruling of the Southern Administrative Central Court, 8 September 2022, Case no 399/22.8BESNT

In the aforementioned decision, the Venerable Judges of the Southern Administrative Central Court - one of the two intermediate instances of the administrative and fiscal jurisdiction in Portugal - ruled that the mere invocation, by the entity to which access to an administrative document was requested (in this case, a public contract), of a regime of restriction of access to information (foreseen in article 6(6), of LADA - Law of Access to Administrative Documents - Law no. 26/2016, of 22 August), without further explanation on how the disclosure of the required information affects the competitive interest and/or the secrecy about the internal life of the company, does not allow, without further ado, to conclude that the disclosure of such information (relating to the execution of the public contract) may seriously affect the competitive capacity or the competitive interest of the company.

According to article 6(6) of LADA, a third party can only access administrative documents containing commercial, industrial or internal company secrets by written authorisation from the company or by demonstrating to hold a direct, personal, legitimate and constitutionally-protected interest that is sufficiently relevant (within the framework of the principle of proportionality, of the fundamental rights in presence and of the principle of open administration) that justifies such access to information - this constitutes a restriction on the right of free access to administrative documents (which includes the rights of consultation, of reproduction and of information about their existence and content - article 5(1) of the LADA).

The said Court considered that, regarding administrative documents with personal data or secrets about the internal life of companies, the public entity must allow the process to be consulted and make available the requested documents, but must remove the information on reserved matters (excluding/hiding the parts relating to matters covered by secrecy). It was also considered that it is the duty of the requested entity to present, on a case-by-case basis, the justification for the concealment of those specific elements, so that the requesting entity may syndicate this action.

SPAIN

edited by

Javier MIRANZO DÍAZ, Professor Lector in Administrative Law at The University of Castilla-La Mancha.

Alfonso SÁNCHEZ GARCÍA, Professor Lector in Administrative Law at The University of Murcia.

ELECTRONIC NOTIFICATION

Central Economic-Administrative Board, Decision of 20th July 2022, proc. 00/05927/2021/00/00.

The case before the Central Economic-Administrative Board addresses the statute of limitations for the settlement of the Corporate Tax of 2016 and the legality of electronic notifications. The core issue in the case before the Central Economic-Administrative Board focuses on the fact that a paper notification was made to an entity obligated to receive communications exclusively through electronic means.

The case before the Central Economic-Administrative Board focuses on the proper execution of electronic notification in the context of the Corporate Tax settlement for the fiscal year 2016. The claimant entity questioned the legality of the notifications made by the Administration, arguing that these did not comply with the necessary legal requirements and, therefore, there was not a valid notification of the verification procedure that would validly interrupt the statute of limitations for the Administration's right to settle the tax.

Initially, the Board establishes that the inspection actions began on October 30, 2018, through a communication notified via the electronic mailbox associated with the entity's enabled electronic address, complying with the stipulations in articles 14.2 and 41.1 of Law 39/2015 of the Common Administrative Procedure of Public Administrations. This law mandates electronic notifications for certain entities, including the claimant in this case.

The central issue of the dispute is the notification of the rectification agreement of the settlement proposal dated June 10, 2021. This notification was made in paper format by a tax agent, despite the entity being obliged to receive electronic notifications. The entity argued that this paper notification was illegal and that it should have been carried out exclusively in electronic format.

In evaluating this situation, the Board considers Article 3.2 b) of Royal Decree 1363/2010, which allows the Administration to carry out non-electronic notifications for reasons of administrative efficiency, especially in situations where the statute of limitations of the Corporate Tax was about to expire and a period for allegations still had to be granted to the taxpayer. In this case, it was considered that the paper notification of the rectification agreement was legit and effectively interrupted the prescription period, as it was made to ensure the effectiveness of the act to be notified and the knowledge of the act by the interested party.

The Board also considered that there was no formal irregularity in the inspection actions. The appropriate procedure was followed in the signing of the act of disagreement, the mandatory deadlines for submitting allegations were granted, and the regulations were followed in the rectification of the proposal. No violation was identified in terms of defencelessness or irregularity that could affect the validity of the notification of the settlement agreement.

In summary, the Board determined that the paper notification of the rectification agreement, although unusual given the entity's obligation to receive electronic notifications, was a measure justified by the Administration to ensure the effectiveness of the notification in a context where the prescription period was about to expire. This decision underscores the flexibility within certain legal limits for the Administration in choosing the method of notification, prioritizing effectiveness, and compliance with administrative procedures.

Contentious-Administrative Court (single judge) number 3 of Madrid. Case 537/2022, 23rd November, appeal number 451/2021

In this case, a penalty for obstruction by the taxpayer is annulled. The case originated from the fact that the taxpayer had not acted in accordance with what was indicated by the Administration through an electronic notification made available to them without the accompanying notice to the email address.

The issue addressed by the Court involves the review of the legality of electronic notifications made by the Administration in the context of a settlement of the Tax on Constructions, Installations, and Works (ICIO, by its Spanish acronym). The focus of the dispute centres on the imposition of a tax penalty on an entity, under the allegation of serious tax infringement due to resistance, obstruction, excuse, or refusal to comply with the administrative action.

The Court specifically analyses whether the notifications complied with the requirements of Article 43 and Article 41.6 of Law 39/2015 of the Common Administrative Procedure of Public Administrations. According to these provisions, electronic notifications must be made through the electronic headquarters of the Administration and are carried out when their content is accessed. Additionally, it is required that the Administration sends a notice to the electronic de-

vice and/or the email address of the interested party about the availability of the notification.

In this case, the Court observes that while the first notification attempt was correctly carried out both electronically and on paper, with publication in the BOE, the subsequent two electronic requirements did not fulfil the obligation to send a notice to the email of the interested party. This omission created a situation in which the interested party was unaware of when the municipal administration would make the notification of the requirement available in the electronic office.

The Court considered that, although the law and its applicable jurisprudence — which we have highlighted in this section of previous numbers of our magazine — establish that the lack of notice does not prevent the notification from being considered valid, in this specific case the absence of notice created a situation of defencelessness for the taxpayer. This defencelessness was considered serious, particularly due to the high fine imposed because of not attending to the requirements. The Court argues that knowledge of administrative acts is essential to exercise the right of defence and that the lack of compliance with a legal obligation, even if it does not have a direct legal consequence, is relevant in the context of the imposed sanctions.

The Court also highlighted the difference in the notification dynamics between electronic notifications and paper notifications, noting that in electronic notifications the recipient must actively access the electronic headquarters of the issuer to obtain the notification. This difference implies that, in the absence of a notice, the taxpayer may not be aware of the need to access the notification, which hinders their ability to respond appropriately.

In the end, the Court concluded that the lack of notice in electronic notifications could not be considered as an intentional non-compliance with the requirements by the taxpayer. Consequently, the two unattended requirements without sending the notice should not be considered for the grading of the imposition of the sanction. Based on this, the Court partially upholds the administrative appeal filed by the sanctioned entity, annulling the originally-imposed sanction and replacing it with a fine of 300 euros.

Constitutional Court. Case 84/2022, 27th June, appeal number 83/2021.

In the present Judgment, the Constitutional Court declares the citizen's right to effective judicial protection to have been violated due to electronic notifications being sent to an electronic address of which the citizen was unaware, and without proper notification of the availability of these notifications, as it was sent to an incorrect address.

The Constitutional Court's judgment examines an appeal related to the legality of electronic notifications in a sanctioning procedure in the land-transport sector. The appeal challenges several judicial and administrative decisions, including a sanctioning resolution and the rejection of a request for ex officio review, brought by a businessman involved in land-goods transport and his legal successor.

The conflict originates when the appellant submits a declaration in December 2016 to the General Directorate of Transport, complying with the requirement of having an electronic address and signature for communications with clients. However, an error occurred in the transcription of his email address in the register, affecting future electronic notifications.

In January 2018, the land-transport inspection requested documentation from the appellant related to the tachographs of his vehicles. The notices of the availability of the notification in the Enabled Electronic Address for this request were sent to the incorrect email address, resulting in the appellant not receiving the notices and failing to respond, leading to the notification being considered automatically rejected due to the lapse of the ten days established in Law 39/2015.

Subsequently, a sanctioning procedure was initiated against the appellant alleging serious infringements related to the driving and rest times of his vehicle drivers. Again, the notices of availability were sent to the wrong email address, preventing access to the relevant notifications.

In October 2018, a fine of €4,001 for each infringement was imposed, totalling €16,004. The defect in the notice of the availability of the notifications of the administrative acts was repeated, so the taxpayer went on without accessing them.

In May 2019, a demand for payment totalling €18,750.53 was notified to the appellant, corresponding to the imposed fines and corresponding surcharges. The appellant requested a review of null acts under Law 39/2015 in relation to the sanctioning resolution, arguing that he had not received notifications at the email address he had provided, but his request was rejected.

The appellant filed a contentious-administrative appeal, invoking the violation of

his right to effective judicial protection and due process, in accordance with Article 24 of the Spanish Constitution. He argued that the notifications of the sanctioning procedure were not correctly carried out due to the error in the email address and that the administration did not exhaust all means to ensure that he was effectively aware of the notifications.

The Central Contentious-Administrative Court No. 5 issued a rejecting judgment, arguing that the error in the email address was attributable to the appellant and that, as a businessman, he should have been aware of his obligation to interact electronically with the administration. The Supreme Court had previously expressed the same view in similar circumstances, as analysed in previous issues of this publication. In the subsequent appeal, the Judgment of October 2, 2018 (appeal no. 38-2018), of Section Seven of the Contentious-Administrative Chamber of the National High Court, confirmed the Court's Judgment. An appeal for cassation was filed, but it was unadmitted by the order of April 11, 2019, of Section One of the Contentious-Administrative Chamber of the Supreme Court.

In the appeal for protection before the Constitutional Court, the appellant alleges the violation of his right to effective judicial protection and the right to defence, attributing it to both the administration and the judicial body. He maintains that the administration did not exhaust all means to ensure that the notifications reached his knowledge and that the judicial body did not give him the opportunity to contradict the administration's arguments.

The State Attorney, in his allegations, dismisses the violation of the right to defence, noting that the appellant notified an incorrect email address and that such action cannot be considered diligent. He argues that, as a transporter, the appellant was obliged to comply with the requirements demanded by the transport regulations, among them, those stipulated in Articles 43 and 56 of the Law on the Regulation of Land Transport.

The prosecution is interested in the partial estimation of the appeal for protection, declaring that the contested administrative resolutions have violated the appellant's fundamental right to defence inherent to the right to due process under Article 24.2 of the Spanish Constitution, given that the sanctioning resolution was issued without enabling the appellant to have effective knowledge of the electronic communication acts.

In this context, the Constitutional Court determines that the fundamental right to defence and to be informed of the accusation of the appellant, according to Article 24.2 of the Spanish Constitution, has been violated.

The Court bases its decision on the finding that the appellant was not effectively aware of the electronic notifications made at his enabled electronic address, as well as the sanctioning procedure that had been initiated. This lack of knowledge was due to the erroneous transcription of his email address in the register, which led to important notifications not reaching his knowledge. The Court considers that this situation generated a violation of the appellant's right to defence, as he could not adequately exercise his rights in response to the ongoing administrative and judicial actions.

Because of this determination, the Constitutional Court decides:

1) To annul both the administrative and judicial resolutions related to this case, including the sanctioning resolution and the decisions of the Central Contentious-Administrative Court, as well as the order that resolved the nullity incident.
2) To order the retroaction of the actions to the moment prior to the electronic communication of the requirement by the land transport inspection. This measure aims to ensure that electronic communication is carried out in a way that respects the fundamental right of the appellant recognized by the Court.

Constitutional Court, First Chamber, case 147/2022, 29th November, appeal number 3209-2019

In the present Judgment, the Constitutional Court finds that the citizen's right to effective judicial protection have been violated due to electronic notifications being sent to an electronic address of which the citizen was unaware, among other reasons, given that the paper notification indicating the implementation of the electronic notification system was delivered to an unsuitable person.

This judgment before the Constitutional Court concerns the legality of electronic notifications and their impact on the right to effective judicial protection of a company in the context of a provisional VAT settlement. The contentious issue stems from an error in the transcription of the appellant's email address in the register of the State Tax Administration Agency. Despite this error, on this occasion, the Court found no violation of the appellant's right to effective judicial protection.

The regulations under analysis refer to the

requirements for the delivery of notifications to legal entities established in the Regulation governing the provision of postal services, approved by Royal Decree 1829/1999. According to this regulation, the notification to the taxpayer of the electronic platform that will henceforth be used for electronic notifications must be made through a paper notification. These paper notifications, when directed to legal entities, must be transmitted to their representative or an employee of the same, and in this case, the initial notification of inclusion in the enabled electronic address system was received by the daughter of the legal representative of the company, a person with no link to the company.

Afterward, once the electronic notification system was operational, the claimant entity did not access the communications sent by the Tax Agency through its enabled electronic address, and therefore was not aware of the initiation and substantiation of the limited verification procedure nor of the provisional VAT settlement for the fiscal year 2012.

In this context, the Court considers that, although the Tax Agency did not breach the current regulations in the way of carrying out electronic notifications, it also cannot be affirmed that the lack of access to the notifications was due to a lack of diligence by the legal representative of the company. Along these lines, the importance of the documentation whose provision was required through the enabled electronic address is also highlighted, as its lack of provision was determinative in the settlement made.

Thus, the decision of the Constitutional Court is based on the interpretation that, although the company had the obligation to receive communications electronically and the Tax Agency complied with the established electronic notification procedure, the specific circumstances of the case, including the manner in which the initial notification was made and the company's lack of access to subsequent notifications, led to violation of the right of defence that could not be attributed to a lack of diligence by the legal representative of the company.

ELECTRONIC APPLICATIONS

Supreme Court, Third Chamber of Contentious-Administrative Matters, Section 4th, case 224/2022, 22nd February, appeal number 806/2020.

The Supreme Court's judgment focuses on a cassation appeal related to the rectification of errors in applications submitted electronically. Specifically, the judgment establishes doctrine regarding the omission of an electronic signature in these applications and the obligation of the Administration to offer the possibility to rectify such errors, granting a period of ten days for this purpose.

The cassation appeal was filed against the judgment of the High Court of Justice of Andalusia, which dismissed the administrative appeal brought by a claimant regarding her exclusion from a selective process due to the lack of electronic signature in her telemetrically-submitted application. The claimant argued that, despite having completed the form and received a message indicating that her application had been successfully processed, the absence of a final step in the electronic submission process led to her exclusion from the selective process.

The Supreme Court, in analysing the case, referred to the applicable regulations, including Article 68 of Law 39/2015 of the Common Administrative Procedure of Public Administrations, which establishes the duty of the Administration to allow the rectification of defects or the omission of documents in any application submitted by citizens. The Supreme Court's judgment overturns the decision of the High Court of Justice of Andalusia and declares the claimant's right to be given a period by the Administration to rectify the lack of an electronic signature and, once the rectification is made, to be included in the employment pools with the inherent effects thereof.

ELECTRONIC AUCTION SYSTEM

High Court of Justice of Catalonia, Contentious-Administrative Chamber, Section 2nd, Case 149/2022, 21st January, appeal number 404/2019.

The judgment resolves on the nullity of Decree 41/2019 of Catalonia, which regulated the creation and operation of electronic means for the conduct of public electronic auctions by the Catalan Tax Agency, as it falls under state jurisdiction.

The judgment of the High Court of Justice of Catalonia concerns the annulment of Decree 41/2019 of Catalonia, which aimed to create a portal for conducting public electronic auctions for the alienation of seized goods and rights in the executive collection period of public revenues of the Generalitat Administration and Catalan local administration entities.

The challenge to the decree was based, first-

ly, on the violation of the constitutional framework for the distribution of competencies in tax matters. The representation of the General State Administration argued that the conduct of auctions is exclusive and must be carried out through the Auction Portal of the State Agency of the Official State Gazette (BOE).

The contested decree was deemed contrary to the constitutional competencies reserved to the State, particularly those established in Article 149.1 of the Spanish Constitution, which include competencies on regulating the basic conditions that guarantee the equality of all Spaniards, the effectiveness of legal norms, the General Treasury and State Debt, and the foundations of the legal regime of Public Administrations and common administrative procedure.

Furthermore, it was pointed out that Article 100 of the General Collection Regulation (Decree 939/05) was also breached, as it stipulates that the conduct of electronic auctions of seized goods must be carried out exclusively through the Auction Portal of the State Agency of the Official State Gazette, not admitting a similar figure at the autonomous community level.

Thirdly, it was argued that the contested decree violated the Organic Law of Financing of the Autonomous Communities (LOFCA, by its Spanish acronym) and the Law regulating the financing system of the Common Regime Autonomous Communities (Law 22/09), which demand absolute respect for state competencies.

Finally, the legality of the regulation was called into question, indicating that the decree failed to comply with the principles of good regulation established in Law 39/15 of the Common Administrative Procedure of Public Administrations, especially the principles of necessity, effectiveness, proportionality, legal security, and efficiency, by creating an unnecessary duplication of public services and generating higher costs.

The Autonomous Community of Catalonia defended its actions, claiming that it acted within its self-organization competencies recognized by the Statute of Autonomy of Catalonia and its Tax Code, denying the violation of the principles of good regulation.

Faced with the litigation thus presented, the High Court of Justice of Catalonia considered that, although Autonomous Communities have the right to seek financial autonomy, they must comply with the norms that take precedence over others, which are those that make up the block of constitutionality, including the Constitution and the laws that distribute competencies between the State and the Autonomous Communities.

Therefore, it was pointed out that the challenged general provisionviolated the exclusive state competencies in tax matters, especially regarding the "General Treasury," allowing the State to fully regulate its own Treasury and establish common institutions for the different Treasuries.

Given the above, the administrative appeal was fully upheld, declaring the contested Decree null and void for being contrary to the General Tax Law, the General Collection Regulation, and the precepts of the laws distributing competencies.

QUALIFICATION OF PUBLIC EMPLOYEES IN THE FIELD OF ELECTRONIC ADMINISTRATION

High Court of Justice of Galicia, Contentious-Administrative Chamber, Section 1st, Case 816/2022, 2nd November, appeal number 222/202

Need for tasks related to electronic administration to be entrusted to personnel with adequate technological training.

The judgment addresses the nullity of a delegation of functions assigned to a public employee. The conflict originates from an administrative decision by the City Council of Lugo, which assigned an employee, with the status of a permanent labour staff member as a psychologist, tasks related to computer duties in the new municipal transparency portal. The CSIF union, representing the employee, contested this delegation of functions, arguing that the tasks assigned were exclusively for career civil servants.

The Court of First Instance estimated the demand, annulling the administrative resolution, considering that the labour employee could not be legally assigned the entrusted tasks, as they were categorized as bureaucratic functions reserved for public officials.

On appeal, the City Council of Lugo argued that the specific tasks assigned in the contested decree should be in the Service of Attention and Citizen Participation, being part of the duties of the employee's job, and that the employee had already been performing similar services under another designation. However, the High Court of Justice of Galicia dismissed the appeal, confirming the judgment of the first instance.

The Court based its decision on the fact that the functions assigned to the employee could not be performed by labour staff, considering his qualification as a psychologist and the digital competencies and knowledge about electronic

administration required for the assigned tasks. It was noted that these tasks were more suitable for those with qualifications related to computer science and new technologies than for a psychologist.

Furthermore, the Court considered that the regulatory norms did not require that the delegated tasks be performed by civil servants, but that the tasks attributed in the contested resolution could not be performed by labour staff due to their technical and specialized nature.

European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 267-270
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 22

Book Review

Elsa Marina Álvarez González: *Regulatory function and legislative technique in Spain. A new tool: artificial intelligence,* Tirant lo Blanch, Valencia, 2022

This timely book collects and analyses relevant digital media cases at the supranational level in Europe,

In Spain, regulatory function is being seriously affected by the accelerated changes currently taking place. With this in mind, Professor Álvarez González embarks on an in-depth analysis of the issues surrounding regulatory function in Spain, and suggests that the key to improving the legislative technique lies in the use of artificial intelligence, an innovative resource that is becoming ever more present in our lives.

In the first section of this work, the author presents an excellent, comprehensive analysis of the disorderly and fragile nature of our regulatory system. We have a serious problem with over-regulation, and this is undoubtedly one of the main reasons why the system of legal sources is so weak, as it calls into question the structural principles of our legal system, including those of legality and the hierarchy of norms. In addition, there is a distinct lack of quality and rationality in our legislative technique regarding norms with the status of law and of regulatory nature. This leads to a violation of the principle of legal certainty and, as the author argues, justifies current public distrust of the political and legislative system.

The second section begins with a study of the regulatory process, in which the author's assessment of its organisation and her focus on the regulatory quality offices is of particular interest. Professor Álvarez goes on to discuss the legislative technique and the factors she considers could contribute to its improvement. Here is where we find the most important and original proposal of this work, namely that of incorporating artificial intelligence into the regulatory process.

Although the use of artificial intelligence is not yet provided for in our legal system, we believe this is an issue administrative law will have to address sooner rather than later, given the progress being made in technological innovations and their application to many sectors of activity, including administrative action. If public administrations can use artificial intelligence to streamline and speed up the processing of administrative procedures and issue reports generated by algorithms based on the data held by a given body, then they can also be useful in the regulatory process.

Artificial intelligence can contribute to better decision-making quality based on a thorough analysis of all the data public administration has at its disposal, as well as existing precedents. Furthermore, artificial intelligence would also contribute to improving the quality of our regulations. Introducing artificial intelligence would involve automating certain procedures in the regulatory process, without, of course, affecting the rights of citizens and groups who play an active role in the process - especially in the prior consultation and public-information procedures.

While artificial intelligence can clearly facilitate the exercise of regulatory powers, its use in the exercise of discretionary powers is a more contentious issue. In such cases, the administration determines the rights, goods or interests that should remain outside the scope of artificial intelligence, such that they cannot be replaced by an algorithm, even if it is technologically possible to do so. In other words, certain decisions should be left to human discretion, a concept that has been referred to as the "reserve of humanity". It is true, however, that the greatest efficiency gains are to be found in discretionary decision-making using artificial-intelligence tools. Here, the transformation is qualitatively different in those areas where increased computational capacity allows for new inferences and a better identification of situations, causes or possible solutions. In this case, efficiency gains are linked to an improvement in the ability to use these tools to evaluate situations, or to take decisions that are different from those that would have been taken, or that are generally taken, by human beings, and that are also not easily anticipated or foreseen by normative and regulatory instruments. And it is in these cases that the greatest risks lie, because the functioning of this type of programme is unknown, in other words, there is a 'black-box effect'. This can prevent programmers from reliably predetermining the specific results of the programme once it has been executed, forcing them to rely, to a certain extent blindly, on the validity of the results based solely

on the assumption that the programming has been carried out correctly. It is here that public law must take a stand and provide a legal response.

Nevertheless, as Professor Álvarez argues, what cannot be left in the hands of artificial intelligence is the will to decide to regulate an issue, and the reasons and justification for doing so, i.e. proposing the regulatory initiative. However, automated administrative action and artificial-intelligence tools could not only speed up certain procedures within the complex regulatory process, but also improve the quality of regulation.

Accordingly, the prior consultation, public hearing and public-information procedures could all be fully automated, as noted above. These procedures channel public participation in the regulatory process and, to date, only electronic means of carrying them out have been regulated. However, we must not lose sight of the power of social networks and platforms to channel information. As such, the author believes that public participation in the regulatory process through social media would generate valuable information and a vast amount of data which, when processed with artificial intelligence, would help public bodies make regulatory decisions.

Applying artificial intelligence to manage citizen participation is not unrealistic. Studies in the US have demonstrated the benefits of using computational analysis to process and evaluate comments and suggestions made by the public during regulatory rule-making procedures. This technology is extremely useful and is deployed when there is massive participation in these procedures and where the officials responsible for processing them cannot reasonably be expected to read and evaluate all the comments posted on social-media platforms and networks.

In short, there are clear benefits to be gained from the use of digital technologies in the regulatory process. These technologies can be used not only to assess public participation but also to interpret the impact of a regulation or the level of compliance with it, as well as facilitate regulatory assessment (both ex ante and ex post), ensure greater regulatory transparency, and even provide information on how to regulate certain situations. This is the conclusion that Professor Álvarez González draws from an exhaustive, innovative and courageous piece of research, which makes a decisive contribution to laying the foundations for a debate on one of the main challenges facing administrative law in our time [reviewed by MANUEL MORENO LINDE].

Luigi Previti, *La decisione amministrativa robotica*, Editoriale Scientifica, Naples, 2022

Scrolling through the tables of contents of the main legal journals, or consulting the relevant databases (for instance, issue 1-2/2020 of this Magazine, dedicated to "The Use of Artificial Intelligence by Public Administration", or issue 2/2020 of Diritto amministrativo), one clearly sees the "uniqueness" of the new monographic work by Luigi Previti, as he himself clearly warns: recently the debate on the technological transformation of the public sector reached a real turning point ["ha raggiunto un vero e proprio punto di svolta"]. In this regard, it is possible to mention, for example, the more than one hundred contributions that the database on the legal documentation of the CNR returns to us when questioned with the query "algorithm" "public": at monographic level, the number of writings is less large, but the relevance of the transformation resulting from technological development, that now leads to the "Algorithmic Society", cannot be underestimated.

It is indeed a decisive change, which marks a turning point not only in the recent history of public digitalization, but also -more generally- in that of the Information Society. Paraphrasing the well-known dialogue between Louis XVI and the Duke of Rochefoucauld-Liancourt, "C'est une révolte? - No, Sire, c'est une révolution", it is no short of a memorable break. Not by chance, also the recent books edited by Pajno, Donati and Perrucci designate artificial intelligence precisely as "revolution" for law (Intelligenza artificiale e diritto: una rivoluzione?, Bologna, Il Mulino, 2022).

Even in the face of the reforms and the investments of the National Recovery and Resilience Plan, which aim (with their own critical issues) at implementing the long-promised "digital administration", the attention of legal scholarship is not devoted solely to e-Government (i.e., the issue of to the provision of digital services and related infrastructure, interconnection, and interoperability) but it is also irresistibly attracted to the only-apparently marginal phenomenon of technology entering the heart of the administrative decision-making process. An indeed, such issue is deeply meaningful: when public decisions are carried out through algorithms, with minimal or no human intervention (e.g. through the use of robotization in procedures), legal scholars do grasp the manifestation of (public) power potentially unchecked by the precautions and protections that the legal system usually (but not yet) provides. Just like in the past adminis-

trative judges, in dialogue with legal scholarship, constrained public power by building banks, and elaborating principles and criteria to balance public functions with the protection of individual rights, administrative law (and not only) is once again in a phase of refoundation, which provides stimulating thoughts for legal scholars. The relevance of the challenge, the complexity of the possible solutions, the magmatic moment, the disorientation (but also the excitement) resulting from the (apparent) lack of applicable legal rules are all elements of a debate that is both intense and also inevitably challenged by the pace of technological evolution, which already forces to face the issues of artificial intelligence, long before having settled the problems arising from variously complex algorithms.

A recent (and only apparently light) Italian movie, directed by Pif, a renown socially-active author , makes us reflect on the entry of "algorithms" into our daily life and their choice-making ability in our relational dimension, work dimension, and overall social dimension. A scenario which, rather than being futuristic and dystopian, is already ongoing and (even worse) not-adequately-regulated. Referring to the inactivity of all who "stood by" while an alienating, insensitive, mechanical, and dehumanizing system took root, the title of the movie prosaically reminds us these processes still remain largely unregulated. In particular, the criticism can be directed against: law-makers (despite initial attempts of a legal framework do exist, also at the European level); independent authorities (although attention to the issue is high, especially by the Data Protection Authority); citizens themselves (who carelessly authorise invasive processing of their data in order to access the increasingly-sparkling services of the Information Society); and public administrations (which seemingly act with excesses of both unpreparedness and superficiality). However, such criticism is not really applicable to administrative judges and scholarship; indeed, thanks to their continuous exchange of ideas and orientations, a framework of algorithmic legality begins to emerge, even if still affected by remaining conspicuous inconsistencies and partial solutions which do not always grasp rapidly-changing phenomena.

At the current crossroad, in between the acceleration of public digitalization and the growth of algorithmic administration, it is inevitable to accept the challenge of the robotization of public power (i.e., not merely predetermined mechanization, but also not-predetermined and complex decision-making resulting from self-learning dynamics and even artificial-intelligence technologies), but at the same time also define its conditions and limits.

In this context, Previti's book joins other monographic works that have recently started to address these issues, in particular; the 2019 book by Giulia Avanzini ("Decisioni amministrative e algoritmi informatici. Predeterminazione analisi predittiva e nuove forme di intelligibilità", Napoli, Editoriale Scientifica); the work of Vinicio Brigante ("Evolving Pathways of administrative decisions. Cognitive activity and data, measures and algorithms", Napoli, Editoriale Scientifica); the book edited by A. Lalli (L'amministrazione pubblica nell'era digitale, Torino, Giappichelli, 2022).

While scholarship on the issues developed, so did the case law, providing new insights and solicitations, even after the "founding" judgments of 2019.

Previti's book joins and develops the debate. It is not a case that the author immediately feels the need to set the factual limits (and the definition) of the phenomenon commonly covering a wide range of manifestations: from "robotization", to "artificial intelligence", passing through the (key, but still somewhat undefined) concept of "algorithm". Herein lies one of the many merits of Previti's book: grasping the need for an approach that, while attentive to legal scholarship, cannot but be interdisciplinary if it is to effectively understand the different situations to regulate. In its recent decisions, also the Council of State deals with the same issue, ultimately distinguishing between simple and complex algorithms, which are sometimes confused with artificial intelligence.

The context, however, is still not well-defined, thereby the challenges of (even scrupulous) judges to grasp the distinction between the concepts, as well as building the necessary taxonomies. Even more though, the real challenge is perhaps understanding a "robotic" reasoning (a reference to the wording of Previti's title) that independently follows its own thinking paths, without overlapping with human ones, as reported in the beautiful work by Kate Crawford (Nè intelligente nè artificiale: il lato oscuro dell'IA, Bologna, Il Mulino, 2021).

This leads us to the heart of the question that stirs the thoughts of those dealing with robotization of the exercise of power (in particular, public power), meaning human ability to control not only the current, but also the possible future technological transformation. Previti opens his work with a quote from Borruso (La legge, il

giudice, il computer, Milano, Giuffrè, 1997), according to whom machines are not free, they only do as they are told ["il computer non è libero, fa solo quello che gli è stato comandato di fare"]; but in reality they are rather "unpredictable" than "free", and the two are not the same. Given the complexity of the phenomenon related to decisions taken "by robots" (including issues arising from simple and complex algorithmic decisions, and AI) the two concepts, in my opinion, often get lost in an area of free choice. An area, however, which is not comparable to a manifestation of individual will, but rather is substantially released, unquestionable, and unfathomable in its elements, as machines grow less and less tied to "what was told".

Two clear examples will suffice: on the one hand, GPT Chat, the new generative artificial intelligence, was commanded to learn and evolve in order to interpret questions and answer problems, even accepting to make mistakes in this path of solution-seeking and self-learning; on the other, nowadays artificial intelligence is asked to create even works of art, whose common (but perhaps soon-obsolete) definition is the typical form of human activity. That alone should be "proof or exaltation of creative talent and expressive ability", therefore the maximum expression of free action. However, this is not the appropriate venue to dwell deeper into this topic.

Previti's book convincingly deals with the ongoing digital transformation leading us in a new era for the public administration; an era where "legal sustainability" (ivi, 167) neither can pass for the zero option of rejecting automation in decision-making processes, nor can reasonably be relegated solely to cases of exercise of constrained powers. However, since such revolution is both relevant and inevitable, it is imperative that the law should set how to limit this power.

There is no straightforward way to do it: Previti persuasively identifies transparency and participation as core protections in algorithmic procedures. However, as the Author convincingly argues, the operative definitions of transparency and participation are not part of the current (that is, "analogical") "toolbox" set forth in the Italian Law of the Administrative Procedure.

Complying with a broad meaning of transparency (towards directly-concerned individuals as well as third parties, as deriving from the general right to access information to increase public accountability) that goes beyond explainability for public decisions is a crucial and complex issue. Doing so will require both the ability to adapt the existing legal framework (also through recourse to analogies and principles that, as Previti underlines, administrative judges already strive to do), as well as the development of new rules expressly designed to regulate this phenomenon [reviewed by ENRICO CARLONI]

Classificazione Decimale Dewey:

340.0285 (23.) DIRITTO. ELABORAZIONE DEI DATI

Printed in March 2023
by «The Factory S.r.l.»
00156 Roma – via Tiburtina, 912



ISSN 2724-5969

ISBN 979-12-218-0798-1

30,00 EURO