EUROPEAN REVIEW OF DIGITAL ADMINISTRATION & LAW

VOLUME 3
ISSUE 1
2022

DIGITALISATION AND GOOD ADMINISTRATION PRINCIPLES

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 1

ERDAL

This volume is part of the project 'Digital citizenship: administrative implications' (TED2021-129283B-I00), won by the University of Oviedo and co-financed by both the Ministero de Ciencia e Innovacion (MCIN/AEI/10.13039/501100011033), and by the European Union NextGenerationEU/PRTR.

ISBN
979-12-218-0078-4

Ist edition
roma 7 July 2023

TABLE OF CONTENTS

Monographic Section: *Digitalisation and Good Administration Principles*

(eds. Emilie Chevalier and Eva Mª Menéndez Sebastián)

Studia Varia

Case Analysis

National Reports

Book Review

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 5-8
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 01

Digitalisation and Good Administration Principles

Emilie Chevalier and Eva Mª Menéndez Sebastián

Digitalisation, algorithms, blockchain, automation, internet of things, metaverse, etc., are terms that have burst into our lives with force in this millennium. However, their use is disparate in the private and public spheres. And this is not accidental, but rather frequent, due to a variety of reasons, including the difficulties of transforming public organisations, the necessary controls, the high cost ...

Like any human activity, the administration has been affected by the digitalisation process. Since the end of the 1990s, digitalisation process has been implemented at the level of States, but also within international organisations, such as the European Union. In this respect, digitalisation has been linked to the promotion of New Public Management,[1] contributing to the reinforcement of the efficiency of the administrations. However, the introduction of new technologies cannot be seen as a purely technical process, reflected in the online availability of information to the administration and the development of electronic means of communication with citizens. Academic work, noticeably in this Review,[2] highlighted and analysed, and is still doing so, how digitalisation has had a profound impact on the administration, and has renewed its organisation and how it operates.[3] *Administration 2.0* is not just an electronic version of the 20th-century administration. It constitutes a renewed framework for the definition and exercise of administrative action as well as for the development of relations between the administration and citizens.

Among the principles of administrative law, the principle of good administration plays a central role. It has been for some decades a fundamental principle for the European administrative area. It is recognized at the level of the European Union, enshrined in Article 41 of the Charter of Fundamental Rights, and recognized or at least implemented within the national legal orders. Good administration is therefore a common standard for European administrations, so much so that it has even been said that this century will be the century of good administration. This notion is defined as the promotion of a quality administration, based on a double dimension, on the one hand an efficient administration, on the other hand at the service of citizens, i.e. able to take into account the expectations of individuals, by guaranteeing the respect of procedural administrative rights, and noticeably impartiality and due diligence.[4] The principle of good administration is therefore a two-sided principle, and good administration expresses a goal, or even an ideal of how the administration should function, based on a balance between these two sides, which may vary according to the times and contexts[5]. Indeed, one particularity of the notion of good administration is its standard nature, i.e. a notion whose content is determined by the actors involved in its implementation, a legislator, an administrative authority or the

[1] See for example, OECD, *The e-Government imperative*, Paris, OECD Publishing, 2003; OECD, *e-Government for Better Government*, Paris, OECD Publishing, 2005.

[2] See for example, A. Barone, A.G. Orofino and J. Valero Torrijos (eds.), *The Use of Artificial Intelligence by Public Administration*, in *European Review of Digital Administration & Law*, vol. 1, 2020.

[3] For some examples, see P. Cossalter, H. Rassafi-Guibal and P. Tifine, *Droit de l'administration numérique*, Paris, LexisNexis, forthcoming, 2024; J.-B. Auby, *Contrôle de la puissance publique et gouvernance par algorithme*, in D.U. Galetta and J. Ziller (eds.), *Le droit public face au défi des technologies de l'information et de la communication, au-delà de la protection des données*, Baden-Baden, Nomos, 2018; E. D'Orlando and G. Orsoni, *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Istituzioni del federalismo*, vol. 3, 2019, 593; D.W. Schartum, *Law and algorithms in the public domain, Etikk i praksis*, in *Nordic Journal of Applied Ethics*, vol. 1, 2016, 15.

[4] J. Ponce Solé, *Quality of Decision-Making in Public Law. Right to Good Administration and Duty of Due Care in European Law and in US Law*, in *European Review of Public Law*, 2009, vol. 21, No. 3, 73.

[5] R. Bousta, *Essai sur la notion de bonne administration*, Paris, L'Harmattan, 2010; E. Chevalier, *Bonne administration et Union européenne*, Bruxelles, Bruylant, 2014.

judge.

The special issue proposes to consider the links and the mutual impact of the simultaneous development, from the beginning of the 21st century, of good administration and of the process of digitalization. Indeed, their respective developments interact to a large extent. The new technologies are one more tool in the hands of the public sector, which must enable it to better address its service to citizens. From this perspective, the connection between technological disruption and good administration is evident. This must be the objective of the use of artificial intelligence and, in general, of the digital transformation in which public administrations are immersed.

Several paths can be followed to explore those interactions. First, it is interesting to focus on the conditions for exercising discretionary power. In the context of digitalization, the exercise of the administration's discretionary power is subject to certain pressures. The development, for example, of automated decisions tends to constrain, or even put aside, discretionary power. Digitalisation thus renews the methods of exercising discretionary power, perhaps limiting it, whereas the principle of good administration requires that individual situations be duly taken into account, in particular in compliance with the due diligence requirement. In what way then does the confrontation of good administration with new forms of digital administrative action have an impact on the meaning and exercise of the administration's discretionary power?[6]

Secondly, digitalisation reinforces certain dimensions of good administration: openness, transparency, efficiency and accountability. The use of new technologies is a source of new areas of interaction between the administration and citizens. Furthermore, the digitalization of the administration tends to renew the ways in which administrative action is legitimized, and the use and implementation of discretionary power. It can help to develop more collaborative and open methods and thus contribute to the promotion of administrative citizenship.

Finally, the principle of good administration can also be mobilised to guide the accountability of the process of digitalisation of the administration. Indeed, digitalisation is not an end, but a means to an end, which is to improve the quality of administrative action. The principle of digitalisation is rarely discussed as such, but perhaps in view of the upheavals it brings, it could be. Can the principle of good administration then serve as a compass, a guide in the conduct of reforms promoted by digitalisation? Thus, it is necessary to assess changes in the way the administration operates, particularly regarding its values, and the balance to be struck between efficiency and the protection of fundamental rights. Does the development of digital administration offer new ways in this respect, or on the contrary, does it only reproduce, or even accentuate, the classic difficulties and obstacles of the implementation of the administrative decision-making process? Good administration is a moving and adaptable concept, capable of integrating new expectations, but it must not lose its meaning, or its mind, with those evolutions. Should there then be limits to its adaptation?

The administration is therefore undergoing transformations, not without important challenges, which administrative law must face, and on which this monograph reflects.

Firstly, Prof. Isaac Martín Delgado illustrates the challenges of automation in public administration, how artificial intelligence, after offering a definition of it, can contribute to the improvement of the administration, but being aware of its limitations, of its current state in the public sector, of its rather complementary nature to human action and especially of the fact that it is a means and not an end. Moreover, it rightly distinguishes between material and formal activity and, within the latter, particularly the due administrative procedure. The use of artificial intelligence systems, which must be guided by the principle of good administration, and which cannot be done in any old way, with particular emphasis on algorithmic, internal and external transparency. The author also makes three proposals, such as the principle of minimum autonomous algorithmic activity; the drafting of a specific regulation on the process of

[6] J. Mendes, *Discretion, Care and Public Interests in the EU Administration: Probing the Limits of Law*, in *Common Market Law Review*, 2016, vol. 53, No. 2, 419; M. Oswald, *Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power*, in *Philosophical Transactions of the Royal Society A*, vol. 376, issue 2128, 2018.

adopting software and the transparency of its operation that specifies and reinforces the principles of transparency, impartiality and participation when configuring the system and its action process; and the existence of a specialised and independent supervisory body or authority with the function of approving algorithmic systems and supervising the specific way in which it operates, as well as guaranteeing its correct operation during its life cycle.

For his part, Prof. Juli Ponce analyses a specific and very interesting issue in the use of Artificial Intelligence, both in the public and private spheres, such as digital *nudges*, choice architectures, *hypernudges*, and how these could contribute to the achievement of good administration, obviously, if they are transparent and focused on the general interest, by attending to people with a citizen-centred approach. But it highlights the multiple risks, the manipulation, the possible infringement of rights - some of them fundamental - such as freedom of thought, autonomy of will, and even, at a general level, the democratic system and the rule of law. It also highlights the need to address its regulation proactively and based on the precautionary principle, given the insufficiency that self-regulation has shown, for example, with the prohibition of obscure patterns, which is the aim of the future EU Digital Services Act, and as some American precedents already do. In short, using the best of Artificial Intelligence and avoiding the worst of it.

Prof. Eva Menéndez Sebastián, with the collaboration of Belén Mattos Castañeda, explains in her contribution how the use of artificial intelligence and, specifically, algorithms can contribute to improved decision-making and, therefore, to good administration. To this end, they start with a brief analysis of the very notion of good administration and its various functionalities, among which, for these purposes, the notion of good functioning and improved decision-making stands out. However, this work also highlights the possible risks associated with the use of artificial intelligence in the public sector, such as the digital divide or, especially, algorithmic discrimination, proposing solutions in this regard, such as prior audits, certifications and, above all, transparency.

Next, Prof. Diana-Urania Galetta highlights the various steps to be taken to achieve a 4.0, digitalised, efficient and effective public administration, which responds more adequately to the right to good administration. Diana-Urania Galetta highlights the various steps that need to be taken to achieve a digitised, efficient and effective Public Administration 4.0, which responds more adequately to satisfy the right to good administration, proclaimed as a fundamental right in art. 41 of the Charter of Fundamental Rights of the European Union. In short, how the use of ICTs by administrations can contribute to their improvement, as well as the role that the National Recovery and Resilience Plan could play in all of this. In this way, it analyses crucial aspects such as the dematerialisation of documents, interoperability problems, the role of the civil servant responsible for the procedure, the relevance of quality data in the due diligence required by the CJEU within good administration and, in short, it offers ideas regarding the essential aspects to be taken into consideration in order to achieve a genuine quality digital administration, which does not entail a digitalisation of complexity.

Professor Katrin Nyman Metcalf explains in a very graphic way how e-governance can contribute to the objective of achieving an efficient and effective administration, improving the provision of services, offering personalised, citizen-based and faster attention. In doing so, she gives examples from the Estonian system, one of the countries that is undoubtedly the most advanced in e-governance. The author explains how automatic digital identity and electronic signature, as well as the important interoperability system - also with noteworthy safeguards, such as the identification of the person accessing the data or the footprint that the access leaves - facilitate the widespread use of digital public services. However, he also appreciates the challenges that this transformation faces, not only in relation to data protection, which can certainly be more protected even than in paper format, but also, for example, possible attacks, such as the one Estonia itself suffered in 2007 - hence the relevance of cybersecurity - or even the lack of acceptance by society. However, none of this justifies not moving towards e-governance, but rather avoiding risks as much as possible.

The digital transition is not only a European issue, but a global one. To find out

how this transformation is being carried out in Latin America, Prof. Mirko Maldonado-Meléndez offers us an interesting overview of the subject, and, specifically, in his work he analyses the creation and implementation of the regulatory organisations of digital government in the various Latin American countries, as governing bodies for digital transformation policies. These digital government agencies or secretariats have become true managers of the public policies designed by the executive powers to direct the digital transformation process of their administrations; however, they are not exempt from certain difficulties, such as their dependence on and proximity to the government, which may imply a certain bias, or the infralegal category of their instruments.

Finally, Hanne Marie Motzfeldt explains in detail the use of artificial intelligence in one of the most developed countries in this field, Denmark, how the principles of Danish administrative law are applied (inquisitorial principle, equality, proportionality, etc.), the impact assessment of good administration, the risk approach and the different categories in this respect, such as verifiable information, value estimates, professional assessments, expert estimates or legal valuations, and the measures that must accompany these different types of application of artificial intelligence by public authorities. All this implies important similarities with the provisions of the future EU Artificial Intelligence Act, although with certain differences, especially from the subjective perspective. Therefore, it will be necessary to amend Danish legislation to make it consistent with the future European regulation and avoid duplication and excessive burdens on citizens and entrepreneurs, undoubtedly an important challenge, especially considering that, as the author points out, most of the artificial intelligence systems used by Danish public authorities are high-risk, according to the classification proposed by the European Union.

In short, this technological disruption that is transforming our lives, also from the perspective of the relationship between authorities and citizens, requires studies, reflection and proposals, such as those presented in this monograph, that can contribute to the constant improvement to which we must aspire in the century of good administration.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 9-30
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 02

Automation, Artificial Intelligence and Sound Administration

*A Few Insights in the Light of the Spanish Legal System**

Isaac Martín Delgado
(Full Professor of Administrative Law - Head of the Center for European Studies "Luis Ortega Álvarez" University of Castilla-La Mancha)

ABSTRACT In a context of increasing technologicalisation of the organisation and procedures of our public administrations with a clear impact on citizens' rights, particularly through the use of artificial intelligence, it is convenient to consider whether our legal standards are still valid and to reflect on how to regulate the implementation of this technology in the public sector. With this approach as a premise and taking into account the principle of sound administration, this paper analyses the application of the transparency legal requirements to the algorithmic administrative activity in order to identify aspects that could be improved and adds some considerations that could help to strengthen the transparency of the algorithmic systems.

1. *Introduction*

1.1. *The big challenge for legal scholars*

Artificial intelligence ("AI") is a transformative and disruptive technology that is impacting all areas of society and will continue to do so in the near future, including public sector.[1]

Since it emerged as a scientific discipline in the 1950s, it has evolved, sometimes rapidly and sometimes more slowly, until its recent exponential development, which is due to three main factors: (i) the increase in the amount of available data (AI feeds off data); (ii) the increase in computing power and storage capacity; and (iii) the development of new techniques. However, it is noticeable that the use and implementation of AI is more widespread within the private sector–commerce, financial services, tourism, industry and the media–than within the public sector. This is not new, since it often takes public authorities longer to embrace new developments and public law is less flexible than private law. Nevertheless, it is somewhat surprising that even official documents on AI focus more on business and society than on public authorities.

Public administration also needs a digital transformation and, above all, public authorities must assess how to apply AI tools and techniques to their organization in order to streamline their relationship with citizens, enhance digital public services, and minimize the risks attached to AI.

The previous scholarly analysis on the implementation of ICTs−and, in particular, on the public-sector use of AI−must rise to the challenge and remain close to reality. However, admittedly, this field of study has been pushed into the background until recently. Some have argued that it is highly technical and has little impact on what really matters in administrative law. Interestingly enough, there were pioneering insights by the time AI began to appear and develop, both in Spain and in neighboring countries. In 1984, V. Frosini examined administrative automation as "the embracement by public authorities of the methods and instruments of current information technology with a view to applying them to public administration." This 1984 work includes meaningful insights on each and every one of the challenges that now concern legal scholars: the transformative

* Article submitted to double-blind peer review.
This paper is the written version of the presentation entitled *Opacity of algorithms: traceability, transparency and explainability,* which was given at the Conference *Artificial intelligence and the public sector: challenges, limits and means*, organized by the Pablo de Olavide University of Seville under the coordination of Eduardo Gamero Casado in the context of the Research Project UPO-1381574, *Artificial intelligence and administrative law: general problems and applications in the Andalusian Regional Government.* The research has been conducted within the framework of the activities of the ADA Research Group of the University of Castilla-La Mancha, funded by the European Commission-FEDE, and the Research Project *Public Administration and Artificial Intelligence: regulation and implementation of AI in the field of public procurement* (TED2021-130682B-I00) founded by the Spanish Ministry for Science and Innovation.

power of software-managed information; the much-needed reshaping of civil service and the re-organization of tasks and duties; the translation of legal code into computer code; the transparency of administrative action; the liability for machine malfunctioning; and the review of automated or computer-based administrative activity, along with the potential risks attached for the legality principle, individual rights and the independence of public authorities from businesses, considering that the powerful tend to get more powerful, even if they incur in wrongdoing.[2] The studies by A. Massucci and G. Duni in Italy were also groundbreaking and remain current.[3]

The greatest challenge at this point is to find the links and connections between AI and public administration. Then, we must ask ourselves a twofold question about how these new technologies can help and whether our set of administrative law rules remains applicable and useful or we must create a new one. To address these questions properly, the starting point must be our current practical reality and the state of the art. We should ask realistic questions, not futuristic[4] ones, searching for useful answers in this context.

In fact, "legal scholars cannot be oblivious to these realities, which are not mere speculation about imaginative futurism."[5] We must approach AI in a realistic and demystified manner, considering AI's current features, since speculating about the future–apparently more interesting than down-to-earth views–cannot be at the expense of being distracted from the important policy issues raised by AI technology today.[6] This scholarly view should also be fair and unbiased, because algorithms are not good or bad *per se*. The actual and potential effects of algorithms depend on their application.[7] In this regard, it is necessary to keep in mind that a significant number of AI projects end up as prototypes and simulations that cannot be applied or implemented for several reasons, including their high cost or the ethical and legal implications;[8] also to note that, as a matter of principle, digital government can work in the same way as traditional government.[9] On top of this, AI is not as developed as to be considered intelligence *stricto sensu*; the results and outcomes delivered by the AI systems that are being created in the public sector field are useful, but not intelligent. Undoubtedly, these useful outcomes are relevant and remarkable, mostly because they

[2] V. Frosini, *Informática y Administración Pública*, in *Revista de Administración Pública*, No. 105, 1984, 447 ff. Also at this time there were approaches that warned about the use of computers. See T.-R. Fernández, *Jurisprudencia y computadores*, in *Revista de Administración Pública*, No. 64, 1971, 327-336. The approach can be summarized as follows: "Reading this (i.e., a computerized case law project) is terrifying. Major issues like applicability or interpretation are going to be solved by a computer, who will decide which rule to apply, which pieces of legislation remain in force and which provisions have been repealed" (p. 331). The author concludes with a warning: "I do not categorically deny that computers may be valid and helpful in this field (time and third-party experiences will tell, while drawing specific boundaries). However, we must now point to the risks and concerns to mitigate this wave of *a priori* enthusiasm and naive pro-machine optimism, particularly in such a legally formalistic country like Spain" (p. 335).

[3] G. Duni, *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e dei procedimenti amministrativi. Spunto per una teoria dell'atto emanato in forma elettronica*, in *Rivista amministrativa della Repubblica Italiana*, No. 129, 1978, 407 ff.; A. Masucci, *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Naples, Jovene, 1993.

[4] There are articles taking this futuristic approach, discussing if there will be fundamental rights in an AI-dominated world when individuals be sidelined or if algorithms should be granted rights. See e.g., E.J. Urbina Mendoza, *El Derecho público del algoritmo. Reflexiones sobre la transición de la modernidad jurídica crítico/lineal a la cuántica/fractal*, in *Revista de Derecho Público*, No. 161/162, 2020, 11 ff.; and G. Osés, *Algoritmos con derechos*, in *Diario 16*, 8 December 2020, available at https://diario16.com/algoritmos-con-derechos. The author claims that algorithms are 21st century slaves and should be granted rights. These works contribute to the reflection on the future that can result from the public-sector use of AI, but they are not really helpful from a regulatory perspective. This paper does not embrace that approach.

[5] The quote is from J.L. Villar Palasí, who wrote it, along with the following, in 1978: "Right now this is not about futurism, but rather about a current issue with ample room for development." See J.L. Villar Palasí, *Aspectos jurídicos y políticos de la Telemática*, in *Revista Española de Derecho Administrativo,* No. 19, 1978, 501. This scholarly article also stresses the potential risks of new technologies, focusing on the loss of fundamental freedoms (p. 502).

[6] H. Surden, *Artificial Intelligence and Law: An Overview*, in *Georgia State University Law Review*, No. 35, 2019, 1306-1307.

[7] H. Fry, *Hola mundo. Cómo seguir siendo humanos en la era de los algoritmos*, Barcelona, Blackiebooks, 2019, 4.

[8] A. Fernández Gil, *Introducción* to M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas)*, Cizur Menor, Aranzadi, 2021, 13.

[9] A. Huergo Lora, *Una aproximación a los algoritmos desde el Derecho Administrativo*, in A. Huergo Lora (ed.), *La regulación de los algoritmos*, Madrid, Thomson-Aranzadi, 2020, 26.

often allow to achieve results that are beyond the human mind.

1.2. *A few preliminary questions*

Modernizing or innovating public administration through technology is not only about technology or law. It requires an all-encompassing and multidisciplinary approach, without any preconceptions or biases, based on an opening question: If they are allowed in the private sector, why shouldn't we bring technological developments into the public sector? Asking this question does not entail overlooking the major differences between both areas for the purpose of implementing AI developments. Rather, the question is aimed at highlighting that public authorities are not being efficient with the large bulks of data they generate, collect and store in the discharge of their duties, seeking to fulfill individual rights and pursuing general interest objectives.

On top of this, we need a second opening question: What would be the point of incorporating disruptive technologies and their transformative power into the various levels of government or public administration? This question does not refer to the overall purpose, but to the aims in the specifics. A quick glimpse shows that public authorities are starting to use these tools when they exercise their powers to limit or restrict individual rights, i.e., for enforcement purposes, and not really for the benefit of citizens. For instance, in Spain, Royal Decree-Law 2/2021, of 26 January, on Employment Protection, provided for automating penalties. As a result, the Employment Penalties and Infringement Act allows public authorities to issue inspection reports in an automated manner.[10] This has been further implemented by Royal Decree 688/2021, of 3 August, amending the Regulation on penalties for employment-related infringements and records for social security settlements. So, right now, public authorities can initiate sanctioning proceedings that be processed in an automated manner all along, until a penalty is imposed for an infringement, provided that the party concerned does not appeal or otherwise challenge the penalty. During all these proceedings there is no human intervention at all.

There is no doubt that public authorities are responsible for monitoring and enforcing infringements, but there is more to it. Assuming that the public administration (i.e., broadly, government) is a social organization serving the general interest, we must demand that innovation be aimed at (i) fulfilling citizens' rights and interests; and (ii) providing public services as efficiently as possible, since this is what justifies government's existence. The principles of effective public service, simplicity, transparency and proximity, laid down in Article 3(1) of Act 40/2015, of 1 October, on Public Authorities ("LRJSP"), do not only refer to penalties, taxes or social security inspections. Public authorities are legitimate vis-à-vis individuals (citizens) by being helpful to them. If public bodies are useless, what role would be left for them and how would they be considered in a context where intermediaries tend to disappear? Just like the *homo digitalis* entails a major change in the way humans interact with the world around them, there is a real risk that digital citizens end up regarding public authorities as an obsolete burden from the past which is completely unnecessary in a post-digital revolution world.

Having asked about why we should incorporate AI into the public sector, and the ultimate purpose thereof, there is a final preliminary question connected with the other two: How should we use AI for government-citizen relationships? AI promises absolute objectivity and effectiveness, but its implementation can be at the expense of citizens' freedoms. Algorithmic determinism,[11] absolute enforcement, serving the general interest rapidly and effectively, with no mistakes or shades of gray, and full legal certainty, are all appealing notions. However, to what extent are they compatible with freedom construed as free individual self-determination under Article 10 of the Spanish Constitution?

[10] For a comprehensive analysis, see J.M. Goerlich Peset, *Decisiones administrativas automatizadas en materia social: algoritmos en la gestión de la Seguridad Social y en el procedimiento sancionador,* in *Labor*, vol. 2, No. 2, 22-42. See also, A. Todolí Signes, *Retos legales del uso del big data en la selección de sujetos a investigar por la Inspección de Trabajo y de la Seguridad Social*, in *Revista Galega de Administración Pública*, No. 59, 2020, 313-337.

[11] J.M. Lasalle, *Ciberleviatán*, *El colapso de la democracia liberal frente a la revolución digital*, Barcelona, Arpa, 2019, 78.

Taking a different perspective, which could be considered "internal," we have noticed that law, i.e., legislation, has clearly lost its once prominent guiding role in the implementation and application of AI systems by public authorities. This is because (i) both at an EU and domestic level, authorities focus on guidelines, strategies and ethics rather than on regulation; and particularly because (ii) law is sometimes regarded as an obstacle than can hinder AI's transformative potential. In practice, algorithms can replace legal provisions,[12] either by action or omission. They would replace legislation by action if lawmakers willingly decide to take a *lawless* approach to the public-sector use of AI, to the requirements applied to the design of algorithmic systems or to the guarantees of citizens' rights, letting ethics and self-regulation take over. Algorithms would replace legislation by omission if lawmakers and governments fail to exercise their regulatory and decision-making powers.

In sum, given the increased use of different technologies for law enforcement by public authorities, it is safe to say that the role of computer programming and software must be under a careful study−and even subject to regulation−thus being essential to carry out an in-depth analysis of all the related challenges. We must not overlook the fact that computer code can interfere with legal code.[13]

We are undergoing a digital transition, with very few rules specifically designed to tackle the challenges posed by disruptive technologies, which is confusing and creates legal uncertainty about how to solve the issues before us. This is why academia must rise to the challenge.

Based on these premises, the analysis provided below focuses on formal administrative activity within administrative procedures. Admittedly, AI can be both useful and risky in other areas of administrative action. However, administrative procedure is the best testing ground for the hypotheses included in the above premises. Note that administrative law is mostly made up of procedures, and many of its core principles (good faith, impartiality, equity, rationality, accessibility, transparency, accountability or participation) are procedural in nature.[14] On top of this, ICTs' main transformative effect impacts decision-making procedures. Therefore, we must (i) rethink our legal categories and regulatory parameters; (ii) appropriately assess which of their features must be strengthened to preserve our achievements in terms of the legality and legitimacy of administrative action vis-à-vis citizens and in the fulfillment of general interest objectives; and (iii) determine whether we need new principles and safeguards.

More specifically, in order to put into practice this approach to administrative law-AI relationships, our insights and analyses will focus on one (major) requirement regarding the implementation of AI in administrative activity: transparency. But first we will discuss (i) the concept of AI as applied to public administration; and (ii) the relevant framework or context, since both (i) and (ii) bring along major requirements and implications for the subject-matter examined herein.

2. *Concept and context: automating administrative activity*

Gaining a full legal understanding and ultimately embracing a reality requires a definition that includes the reality's main dimensions, in order to come up with an appropriate legal framework. However, in order for this definition to be a lasting one, it must be flexible enough, particularly if it refers to concepts that evolve very rapidly, like AI.[15]

In simple terms, although there are very different scholarly definitions of AI, we can define this concept as follows: AI is any human-made rational agent that decides and acts based on perception,[16] processing information to deliver an outcome through a

[12] Lasalle rightly points out that "algorithms cannot be the law by default of national legislation," J.M. Lasalle, *Ciberleviatán*, 158.

[13] In line with this approach, see T. Wu, *Will artificial intelligence eat the law? The rise of hybrid social-ordering systems*, in *Columbia Law Review*, vol. 119, No. 7, 2001-2028. See a comprehensive analysis in a specific area of action from this perspective in E. Micheler and A. Whaley, *Regulatory technology: replacing Law with computer code*, in *Law, Society, Economy Working Papers*, No. 14, 2018, 1-28.

[14] C. Harlow and R. Rawlings, *Proceduralism and automation: challenges to the values of Administrative Law*, in *Law, Society, Economy Working Papers*, No. 3, 2019, 2.

[15] In this vein, see M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas)*, Cizur Menor, Aranzadi, 2021, 13.

[16] S. Russell and P. Norving, *Artificial Intelligence, a modern approach*, III ed., Upper Saddle River, N.J, Prentice Hall, 2010, 1-2.

human-like reasoning. What makes AI worthy of the adjective "intelligent" is the ability of perceiving, and even transforming, the environment.

Broadly, AI is a scientific discipline comprising several complex techniques–machine learning, automated reasoning and even robotics–which allow to design and implement software and hardware that make decisions or help in decision-making based on the processing and interpretation of data. Currently, it is hard to understand intelligence as human intelligence, i.e., having human-like skills.

A meaningful analysis of algorithms and administrative action requires examining the concepts and the implications of using them within the scope of public administration.

Merriam-Webster's Dictionary defines algorithm as a "step-by-step procedure [involving a finite number of steps that frequently involves repetition of an operation] for solving a problem or accomplishing some end." When applied to the field of AI, algorithms perform the same function although based on logical instructions or commands translated into computer code[17]–where these instructions are either fully created by humans and operate directly and unambiguously, or partially generated by the system–but without understanding the information they handle as a human being would. In fact, depending on the task, it is irrelevant whether the machine understands the knowledge that is being generated. What really matters is that the machine's probabilistic or statistical approach stemming from the computer processing of large datasets be suitable for the end pursued. So, the more codifiable the processes, the more efficient and useful the algorithmic systems will be. And, precisely because of this, in order to truly understand the system's underlying rationale, we need to learn its real objectives.[18]

Algorithmic administrative action primarily refers to the activity performed through systems that involve algorithmic processes to automate human decision-making,[19] whether totally or partially.[20] This definition would include both fully programmed automation and the use of AI *stricto sensu*. However, we must draw a distinction between the two. In the first case, the machine's output expresses the human will, anticipated through previous programming (thus being a different way of expressing a will, since the programming responds to the programmer's commands), summarizing regulatory criteria, turned into algorithms, and leading to the final decision through a predetermined logical and conditioned sequence. In the latter case, it is not merely about programming. Rather, it involves "thinking," i.e., the ability to form a judgment or an opinion about something, and to follow autonomous intellectual processes.[21] In fact, machine learning allows to generate predictions or forecasts through self-learning systems, and learning is a sign of intelligence because it is required to be intelligent.[22] These algorithms are not deduction-based. Rather, they make probabilistic predictions. Therefore, they are more capable of representing the real world.

Nevertheless, we are discussing programming, and thus the optimization of systems to accomplish specific goals based on data and sorting processes. Simply put, their huge potential to generate knowledge is offset by blatant "narrow perceptual abilities."[23] However, these systems can have such a tremendous impact that could end up having more significant effects on society than human-made decisions, since these human-

[17] L. Lessig, *Code and other laws of cyberspace*, New York, NY, Basic Books, 1999.

[18] D. Cardon, *Con qué sueñan los algoritmos*, Madrid, Ediciones Dado, 2018, 81.

[19] J. Cobbe, *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making*, in *Legal Studies*, vol. 39, 2019, available at http://dx.doi.org/10.2139/ssrNo. 3226913, 3.

[20] A. Huergo Lora makes a difference between automated administrative action and algorithmic predictions. In his view, there is automated action without AI, just like there is AI that does not involve automated action. He is right. However, in this paper, the term automation is used to mean the reproduction of intellectual processes by machines through information systems, regardless if they are used to adopt administrative acts or decisions–whether final or non-final procedural resolutions–or to obtain relevant information based on data. See A. Huergo Lora, *Administraciones Públicas e inteligencia artificial: ¿más o menos discrecionalidad?*, in *El Cronista del Estado Social y Democrático de Derecho,* No. 96-97, 78-95.

[21] "Algorithmic system," "IA system" or "algorithm" are used interchangeably in this paper to refer to human-designed software in order to solve problems by interpreting data.

[22] A.M. Turing, *Computing Machinery and Intelligence*, in *Mind*, No. 59, 1950, 433 ff.

[23] D. Cardon, *Con qué sueñan los algoritmos*, 13, 21 and 58.

manufactured systems shape us, because they have the ability to organize and steer our reality. In other words: what is real becomes more easily manipulated.[24] There is a second negative impact related to this large computational capacity: the exponential increase in the amount of data exceeds human assimilation, which makes machines indispensable, thus making us overly dependent on them.[25]

Ultimately, we are experiencing a transformation process in which there are fewer human decisions relying on human-obtained information. These decisions are being replaced by decisions based on machine-provided information. This process also affects public authorities.

In this context, note that the concept of AI refers to the technology that makes machines "intelligent," reproducing or imitating some human intellectual skills. This has many potential applications, e.g., robotics, process automation or decision-making. A set of algorithms is a code, a sequence of instructions for problem solving that transforms data into knowledge in order to make decisions. An algorithm's main functionality is that it "letting the data speak"[26] because it searches for data and identifies action patterns and correlations between the data and the desired outcome. In sum, machines learn to generate data-driven descriptions, predictions and prescriptions– and thus knowledge. The decision is not made by a program based on certain algorithms. Instead, the decision is explained by the data or, in other words, the decision gives meaning to the data.[27] Not all legal problems can be solved with algorithms, because many legal issues require intuition and not only analytical abilities.[28] But administrative law leaves much room for factual administrative action (e.g., controlling traffic through AI-powered traffic lights, drone surveillance of public areas, road surface marking or land surveys for expropriation purposes) and formal activity (e.g., deciding which companies must be subject to tax inspections, appointing public officials to regional bodies, awarding subsidies or monitoring regulatory non-compliance risks), which can be optimized through algorithms.

So, keep in mind that there are various types of administrative activity and different scopes of application. For now, we will focus on three main forms of administrative action: (i) regulation or rulemaking; (ii) the adoption or issuance of administrative acts (discretionary and non-discretionary or mandatory); and (iii) factual activities in the exercise of administrative powers (like inspection, organization of work for public officials or disclosure of information to fulfill transparency requirements). Accordingly, the scope and role of algorithms will differ depending on the type of activity. Therefore, any analyses or reflections on AI-public authorities relationships cannot be made broadly. It is essential to draw a distinction between areas of action, since there are many fields that could be automated: there is a difference between automating formal activities (e.g., a public tender) and providing public services (e.g., diagnosing diseases). Assuming that using AI systems is a choice, it is for scholars, lawmakers and the Government, along with legal and technical stakeholders, to identify AI's and algorithms' role. Algorithms can be used to make decisions or simply to support human-made decisions. As for decision-making, they can be used to exercise close-ended powers or prerogatives with little scope for discretion.[29] However, let us recall that algorithms may also be used to create, apply, enforce and amend rules.[30] Law can be partially

[24] A.M. Turing, Computing Machinery and Intelligence, 433 ff.

[25] J.M. Lasalle, *Ciberleviatán*, 40-43.

[26] K.K. Yeung, *Algorithmic Regulation: a Critical Interrogation*, in *Regulation & Governance*, 2018, 12, 506.

[27] As pointed out by Huergo Lora, the application of predictive algorithms supersedes subjective decisions, that are replaced with predictions based on correlations that have been found by analyzing large datasets regarding past operations. However, at the same time, predictive algorithms also set aside rational criteria, because these predictions replace causality with correlation. See A. Huergo Lora, *Una aproximación a los algoritmos desde el Derecho Administrativo,* 35.

[28] V. Frosini, *Cibernética, Derecho, Internet y Sociedad*, Santiago de Chile, Ediciones Olejnik, 2019, 88.

[29] I. Martín Delgado, *Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada*, in *Revista de Administración Pública*, No. 189, 2009, 353 ff.

[30] L.B. Solum, *Artificially Intelligent Law*, in *Rivista de BioDiritto*, 1, 2019, 53 ff.; D. Canals, *El proceso normativo ante el avance tecnológico y de la transformación digital (inteligencia artificial, redes sociales y datos masivos)*, in *Revista General de Derecho Administrativo*, 50, 2019. In this regard, M. Moreno Rebato specifies that the ability of the existing computer codes to translate legal provisions into

computerized, and the application of AI focuses on accurately describing learning processes and other features of human intelligence so they can be reproduced by a machine.[31]

This calls for an in-depth analysis and discussion on the types of administrative powers and decisions that can be exercised and adopted using algorithms. We must also reflect on how to ensure that the legal language is being faithfully translated into computer code, i.e., accurately reflecting the lawmaker's intent and purpose. This is essential, because code writers interpret legal norms when they translate it from human language to computer language and therefore can make mistakes or there can be distortions.[32] Indeed, programmers and code writers do not only design software, but also build decision-making systems from a legal perspective.[33]

The materialization of all these challenges has a twofold link. On the one hand, they must abide by the principle of sound administration. On the other, they are subject to the principle of transparency.

3. *Grounds: the principle of sound administration*

After summarizing the concept of AI and its implications for administrative law, as well as the context for its application, it is worth providing an overview of the grounds, i.e., the "pretext," for using AI systems.

The term pretext should not be construed as having any negative connotations. Self-evidently, public-sector use of AI is not an obligation but an option. Nevertheless, it becomes an indispensable option if we take the principle of sound (alternatively expressed as "good") administration seriously, i.e., a general principle governing public authorities' activity that has been acknowledged as a set of individual rights.

Sound administration must be the principle that guides the use of AI in administrative organization and procedure. This is yet to be fully internalized or assimilated by public authorities.[34]

A good public administration is made up of public authorities that perform the duties allocated to them, doing so in a transparent manner, serving citizens impartially, rationally and giving reasons for their decisions. ICTs–and AI in particular–can effectively secure the principle/right of/to sound/good administration.[35]

From a dogmatic perspective, administrative procedure under Spanish law is an autonomous, stand-alone constitutional institution or construct with a threefold purpose: (i) an instrument aimed at serving the general interest; (ii) a means for ensuring that public authorities act in accordance with the principle of legality; and (iii) a means for citizen participation in administrative decision-making.

This threefold purpose is enshrined in the Spanish Constitution, from which a set of principles and rights applicable to administrative procedures stem. The administrative procedure thus qualifies as an instrument to fulfill the relevant constitutional principles and standards related to administrative or public authorities' action.

First, Article 9(3) of the Spanish Constitution precludes arbitrariness, i.e., it states the principle of prohibition of arbitrariness. Art. 31 provides for the efficiency and rationality standards in public spending, and Art. 103 is worded as follows: "The public Administration serves the general interest with objectivity and acts in accordance with the principles of efficiency, hierarchy, decentralisation, deconcentration and coordination, being fully subject to justice and the law." On top of this, the Constitution

computer code for decision-making must not interfere with or otherwise restrict the exercise of lawmaking and rulemaking powers. However, he also claims that in a near future it is likely that legal rules be drafted in two formats: (i) human or natural language; and (ii) computer language, thereby enabling their full application and enforcement: M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas)*, 129.

[31] S. De la Sierra, *La matematización de la realidad y del Derecho Públic,* in *Ibericonect*, 14 March 2022, available at www.ibericonnect.blog.

[32] D.K. Citron, *Open Code Governance*, in *University of Chicago Legal Forum*, No. 1, 2008, 366-367.

[33] D. Hogan-Doran, *Computer says "no": automation, algorithms and artificial intelligence in Government decision-making*, in *The Judicial Review*, No. 13, 2017, 8.

[34] J. Ponce, *Inteligencia artificial, Derecho administrativo y reserva de humanidad; algoritmos y procedimiento administrativo debido tecnológico*, in *Revista General de Derecho Administrativo*, No. 50, 2019, 6.

[35] D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione (il procedimento amministrativo, fra Diritto UE e tecnologie ICT)*, in R. Cavallo Perin and D.U. Galetta (eds.), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino, Giappichelli, 85.

instructs lawmakers to pass legislation regulating the impartiality standards applicable to public officials in the discharge of their duties.

The administrative procedure is thus the formal means enabling public authorities to (i) fulfill the public needs provided in the Constitution and the relevant statutory provisions (laws or parliamentary statutes); and (ii) secure the legality principle. Along these lines, according to the preamble of Act 39/2015 on the General Administrative Procedure ("LPAC"), "the citizens' set of rights and entitlements is protected vis-à-vis public action by preventive mechanisms and instruments (...) relying on the administrative procedure, which ultimately expresses and ensures that public authorities remain fully subject to the law." On top of that, as shown below, the objectivity standard for public action has a specific bearing on the administrative procedure.

The Constitution does not expressly provide for the general principle of sound administration. However, both the Spanish legal scholarship and the case law have inferred the requirement of good administration, along with public authorities' legal obligation to conduct fair administrative procedures (due process) and the right to fair administrative procedures (due process right), the purpose being to achieve sound administrative decisions. Therefore, the administrative procedure is no longer construed as a process to adopt administrative acts (that was the 19th century and early 20th century approach). Rather, the procedure is now a means to guarantee good or sound administration.[36]

In its case law, the Spanish Supreme Court has consistently drawn an implied principle of sound administration from various constitutional provisions, in line with Art. 41 of the Charter of Fundamental Rights of the European Union ("CFREU"). Note that Art. 41 CFREU requires that administrative action be conducted or handled with due care or due diligence.[37]

The LRJSP has enshrined into Art. 3 various general principles and standards governing public authorities' action. It is worth noting the principles of participation, objectivity and transparency, along with the duty of good faith, the principle of legitimate expectations and the principle of institutional loyalty. Article 3 LRJSP only mentions these principles, without further specifying their content. Also, the Supreme Court has drawn from this provision the principle of good or sound administration.[38]

Finally, it is worth highlighting a general idea discussed above. Art. 75 LPAC is worded as follows: "[A]ny investigative acts required to determine, verify and establish the facts of the case shall be conducted ex officio and electronically by the body or authority conducting the procedure. This is without prejudice to the stakeholders' [concerned parties'] right to request any acts or proceedings (i) requiring their participation; or (ii) qualifying as statutory or regulatory requirements." This gives rise to the due process right to a fair procedure, thereby

[36] See J. Ponce Solé, *Deber de buena administración y derecho al procedimiento administrativo debido. Las bases constitucionales del procedimiento administrativo y del ejercicio de la discrecionalidad*, Valladolid, Lex Nova, 2001 and, more recently, Id., *La lucha por el buen gobierno y el derecho a una buena administración mediante el estándar jurídico de diligencia debida*, Alcalá de Henares, Universidad de Alcalà, No. 15, 2019. Taking a specific approach regarding the use of AI systems, see also J. Ponce Solé, *La prevención de riesgos de mala administración y corrupción, la inteligencia artificial y el derecho a una buena administración*, in *Revista Internacional de Transparencia e Integridad*, No. 6, 2018, 1-19.

[37] See an example of this in the Supreme Court Judgment of 15 October 2020: "The principle of sound administration is implied in Articles 9(3), 103 and 106 the Spanish Constitution. Also, it was codified in Articles 41 and 42 CFREU (...) and, according to the prevailing scholarly opinion, it shifted the 21st century legal paradigm bringing a new approach to public action precluding negligent management (...). As noted by this Court before, the principle of sound administration is not an empty shell. In fact, it is imposed on public authorities so that the set of rights and entitlements arising therefrom (the right to be heard, timely adjudication, reason-giving requirements, the requirement to conduct the proceedings and adjudicate the cases fairly or the duty of good faith), along with the relevant requirements incumbent upon public authorities, be effectively enforced."

[38] Supreme Court Judgment of 19 February 2019 provides the following: "We have already discussed the principle of sound administration implied in Articles 9(3) and 103 of the Constitution, found in many rulings and codified in Article 3(1)(e) LRJSP. This principle requires public authorities to act as diligently as to prevent possible maladministration. It does not suffice for public authorities to strictly comply with the relevant procedural requirements. Rather, the principle of sound administration (i) requires that all statutory and constitutional rights and safeguards be secured and duly provided to taxpayers [i.e., citizens]; and (ii) instructs tax authorities to act with due care so as to ensure the effectiveness of these rights and safeguards whilst guaranteeing appropriate legal remedies preventing unlawful profits."

requiring public authorities to act rationally and to make reasonable and sound decisions, as boldly stated by the Supreme Court in its Judgment of 14 April 2021.[39]

In a nutshell: administrative procedure–along with the statutory proceedings and safeguards attached thereto–is the means for enforcing the principles of sound administration, transparency and participation provided in the Constitution.

This overview of (i) the implications and requirements that flow from the principle of sound administration in connection with administrative procedure; (ii) the statutory provisions that enshrine such implications and requirements; and (iii) their respective scopes in Spanish case law, allows for a better understanding of an idea that has already been anticipated: the public-sector use of AI contributes to fulfill this ideal, but it has to be done in a certain way.

Public authorities must be understandable when taking AI-driven action,[40] which triggers the need for reviewing and tightening, if appropriate, any transparency and reason-giving standards or requirements. However, on top of this, we must not overlook a clear connection with the principle of sound administration: carrying out or processing an administrative procedure to use an AI system[41] is necessary to secure transparency (disclosure), participation (legitimacy) and legality (impact assessment).

These legal safeguards must be brought to the foreground and, when appropriate, incorporated into an all-encompassing approach also comprising political science outlooks.[42] For now, this approach can be summarized as having the following (essentially overlapping) aspects: systems (i) should be carefully designed by multidisciplinary teams; (ii) must be previously evaluated by a specialized certification agency; (iii) should be transparent and allow the public decision-makers to justify the decisions they adopt through them; and, in any event, (iv) public AI experts must be involved in the configuration, programming and operation of these systems.[43]

4. *Internal and external transparency of algorithmic administrative action as the materialization of the right to sound administration*

4.1. *Premise*

Based on the above considerations, it is worth concluding that, from a formal perspective, the main challenge posed by the public-sector use of AI systems is transparency related.[44]

The principle of good faith in government-citizen relationships, set out in Art. 3 LRJSP, is closely linked with the principle of sound administration. The transparency principle falls within this context, and can be construed as the possibility of being aware of automated decision-making processes[45] and of their underlying rationale.[46]

[39] See Supreme Court Judgment of 14 April 2021 (Appeal 28/2020): "The due process right to a fair administrative procedure, which is a corollary to the principle of sound administration, ensures that administrative decisions (...) be adopted duly giving reasons and in line with the procedural steps, without any procedural impropriety, since there must be no inconsistencies between the factual background, the legal grounds and the content of the relevant administrative decision. Under this constitutional sound administration requirement (...), public authorities must fulfill the reason-giving requirements and the principles of objectivity, transparency and rationality subject to Articles 35 and 129 LPAC. Within this context, regarding the public authorities' duty to comply with all the procedural safeguards, we find an infringement of the due process right to a fair procedure. This due process right stems from the Constitution, namely from (i) Art. 24, ensuring the right to an effective legal remedy and, generally, the right to effective legal protection; and (ii) Art. 103, providing that all administrative action should be governed by the principle of objectivity."

[40] J. Ponce Solé, *Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico*, in *Revista General de Derecho Administrativo*, No. 50, 2019, 40.

[41] J. Valero, *Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración*, in *Revista catalana de dret públic*, vol. 58, 2019, 88, and J. Ponce, *Inteligencia artificial*, 35.

[42] E. Menéndez, *Buena administración, algoritmos y perspectiva de género*, in P.R. Bonorino, P. Valcárcel and R. Fernández (ed.), *Nuevas normalidades: Inteligencia Artificial, Derecho y género*, Cizur Menor, Aranzadi, 2021, 35-63.

[43] C. Ramió, *Inteligencia Artificial y Administración Pública*, Madrid, Los libros de la Catarata, 2018, 116-117.

[44] J. Cobbe, *Administrative Law and the Machines of Government*, 5.

[45] D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione*, 99.

[46] For a comprehensive approach to the transparency principle related to the use of AI and massive data, including some case studies, see L. Cotino, *Hacia la Transparencia 4.0: el uso de la Inteligencia Artificial y big data para la lucha contra el fraude y la corrupción y las (muchas) exigencias constitucionales,* in C. Ramió

There is a point to make before discussing the transparency of public authorities' actions in the context of the public-sector use of AI systems: human decision-making and action is far from transparent.[47] We have created a formal framework where transparency means disclosing diverse information that is considered relevant for justifying administrative action and for accountability purposes. This formal framework also allows for the possibility of requesting access–under public authorities' scrutiny–to information held by public bodies. The transparency principle definitely applies to algorithmic administrative action, and it poses its own challenges. But we can come up with a set of rights and obligations that allow for accepting the applicability of the principle of transparency to public action with *ad hoc* safeguards.

4.2. *A practical exercise: regulating the transparency of algorithmic administrative action*

There are various ways of tackling transparency-related challenges from a legal perspective. A regulatory perspective could be a good approach and, more specifically, it is worth examining how this matter was dealt with by the Charter of Digital Rights passed by the Spanish Government (note that the Charter was prepared by the State Secretariat for Digitalization and AI with the support of an expert group).[48] This is an interesting approach because it is the first attempt at a general regulation on the subject. Also, it provides a great opportunity to gain a better understanding of the role of law in regulating technology. In sum, this approach allows to test the methodology discussed above.

There is no doubt that the lack of transparency (also referred to as "opacity") is a major risk posed by AI systems. EU documents on this matter[49] lay down three

(ed.), *Repensando la Administración digital y la innovación pública*, Madrid, Instituto Nacional de Administración Pública, 2021, 169-196.
Regarding the Italian system, see A.G. Orofino, *The Implementation of the Transparency Principle in the Development of Electronic Administration*, in *European Review of Digital Administration & Law*, vol. 1, 2020, 123-142.

[47] C. Coglianese and A. Lai, *Algorithm vs. algorithm*, in *Duke Law Journal*, vol. 72, 2022, 1313.

[48] Available at www.lamoncloa.gob.es.

[49] In particular, see *Ethics Guidelines for Trustworthy AI*, in https://op.europa.eu/es, published in April 2019 and prepared by the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission in June 2018 (the "AI Guidelines"). As stated by the AI Guidelines, "[t]rustworthy AI has three components, which should be met throughout the system's entire life cycle: (1) it should be lawful, complying with all applicable laws and regulations (2) it should be ethical, ensuring adherence to ethical principles and values and (3) it should be robust, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm. Each component in itself is necessary but not sufficient for the achievement of Trustworthy AI. Ideally, all three components work in harmony and overlap in their operation. If, in practice, tensions arise between these components, society should endeavor to align them." The AI Guidelines specify the main contents of each of these three cornerstones. Accordingly, lawful AI means that AI must fulfill negative legal obligations (i.e., what cannot be done) and positive obligations (what should be done), which should be founded on fundamental rights (respect for human dignity; individual freedom; respect for democracy, justice and the rule of law; equality, non-discrimination and solidarity and, more broadly, citizens' rights vis-à-vis public authorities); ethical AI involves being aligned with ethical norms arising from the principles of respect for human autonomy, prevention of harm, fairness and explainability; robust AI entails achieving that systems operate safely at a technical level. The AI Guidelines add a series of principles that must be translated into specific requirements to achieve Trustworthy AI: human agency and oversight (assessing the impact on fundamental rights and preserving the autonomy of addressees of AI systems as a guarantee of their operation and results); technical robustness and safety (including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility); privacy and data governance (respect for privacy, quality and integrity of data); transparency (traceability, explainability and communication); diversity, non-discrimination and fairness (including the avoidance of bias, accessibility and universal design, and stakeholder participation); societal and environmental wellbeing (sustainability and an approach aimed at enhancing society); and accountability (system auditability, minimization and reporting of negative impacts, trade-offs and redress.).
The European Declaration on Digital Rights and Principles for the Digital Decade (COM (2022) 28 final, of 26 January) is a more recent document. It was accompanied by a Communication from the European Commission explaining the initiative, which was closer to legal propaganda than to an actual innovative provision in legal terms (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a European Declaration on Digital rights and principles for the Digital Decade, COM (2022) 27 final, of 26 January). The Declaration emphasizes (i) the need to place citizens at the center of the digital transition; and (ii) its applicability to public authorities. However, the Commission preferred to issue a political declaration of rights, and the Declaration itself confesses that not all the principles provided therein bring along directly applicable or enforceable rights. This is a surprising approach for two reasons. First, it conveys the idea that the digital world differs from the physical world.

requirements when it comes to applying transparency standards to AI techniques: (i) traceability (i.e., the capability to keep track of an AI system's data, development and deployment processes, typically by means of documented recorded identification); (ii) explainability or explicability (i.e., the ability to explain an AI system's technical processes and the human decisions attached thereto); and (iii) auditability (i.e., an AI system's capacity to enable the assessment of its algorithms, data and design processes). It is essential to keep track and document the data fed to the system and its operational process, letting stakeholders know how it works and disclosing the system's capabilities and limitations, as well as letting stakeholders participate in the system's design and application.

So, algorithmic systems' opacity can have three distinct forms:[50] (i) legal opacity, i.e., arising from the protection requirements related to other rights and interests (e.g., intellectual property); (ii) sociological opacity, which arises from the little capacity for understanding how the systems work from a technological perspective; and (iii) intrinsic opacity, where a system's complex decision-making process itself is difficult for any human to understand. In my opinion, point (i) is necessary, point (ii) must be steadily remedied or corrected, by seeking to improve public officials' and citizens' technological skills, and the effects of point (iii) could be mitigated by researching and developing the technology itself. However, the form of opacity that law should combat, because it is absolutely unjustified, is the so-called intentional opacity, i.e., the concealment of the use and operation of these algorithmic systems.

We must begin by considering two premises:

– In practice, the AI applications and solutions currently used by public authorities more often than not have not been subject to a formal authorization or approval process. Also, usually they are not acknowledged or well-known except for specific references in press releases or technical documents. This creates opacity, legal uncertainty and mistrust, thus significantly impacting the legitimacy of public authorities' action.

– From a theoretical perspective, the public-sector use of AI systems is an expression of the public authorities' duty to serve the general interest effectively and objectively, as required by Art. 103 of the Constitution. AI can also be used to fulfill the principle of sound administration, which must be reconciled with the rights and safeguards granted to citizens by the Constitution and the rest of the Spanish legal framework. And, in particular, AI must fulfill and secure the individual rights stemming from the principle of sound administration. Therefore, AI is an instrument, not a replacement, of the notion of public administration within the terms of the *Constitución Española*.

On top of that, keep in mind that the use of AI techniques is neither a given nor an imposition. It is us who must determine which instruments are best suited to meet our needs, along with their scope, applicability and safeguards, and we must do so by relying on the law, public policies and technical aspects. An essential safeguard is transparency, tied to the duty to give reasons and to the need for

However, they are both part of our real world, in which we move and interact with other people and public authorities. Second, it is shocking that the Declaration list political intentions instead of (i) regulating new rights to protect citizens against the potential risks of technology and (ii) providing for new obligations to secure these rights. On top of that, the Declaration is declaratory (repetition intended), although all legal texts (including non-binding instruments) are intended to have legal effects. We do welcome that the Declaration (i) seeks a human-centered and value-based digital transition; (ii) provides that technology should have a secondary role and be at the service of citizens and used for their benefit; and, above all, (iii) provides that everyone should have access to all key public services. Chapter III, "Freedom of choice," is particularly interesting. Its first section addresses the interactions with algorithms and AI systems, providing a principle and several political commitments: (i) the principle that everyone should be empowered to benefit from the advantages of artificial intelligence by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights; (ii) the commitment to ensure that algorithmic systems are based on suitable datasets to avoid unlawful discrimination and enable human supervision of outcomes affecting people; (iii) the commitment to ensure that algorithms are not used to pre-determine people's choices, for example regarding health, education, employment, and their private life; and (iv) the commitment to provide for safeguards to ensure that artificial intelligence and digital systems are safe and used in full respect of people's fundamental rights.

[50] J. Cobbe, *Administrative Law and the Machines of Government*, 5. Along these lines, A. Cerrillo, *El impacto de la inteligencia artificial en las Administraciones Públicas: estado de la cuestión y una agenda*, in A. Cerrillo i Martínez and M. Peguera Poch (eds.), *Retos jurídicos de la inteligencia artificial*, Cizur Menor, Thomson Reuters Aranzadi, 2020, 83-84.

appropriate review or scrutiny.

As discussed before, transparency is both a general principle guiding administrative action (set out in Art. 3 LRJSP) and a constitutional right (provided in Art. 105 of the Constitution and further implemented through the Act 19/2013, of 9 December, on Transparency and Good Governance or "LTBG"). Both as a principle and as an enforceable right, transparency has many dimensions and practical applications in various areas of the administrative law framework, but they are all dimensions of the same principle and of the same right. Explainability, i.e., the ability to explain technical processes and the decisions arising therefrom, is essential to build trust in the algorithmic system,[51] but even more so to allow for the legal acknowledgement of algorithmic systems if they are used for decision-making. In fact, the human ability to interpret the system's technological process is tied to the duty to give reasons, insofar as it allows for explaining the factual context or the factual grounds of the decision.[52]

Consequently, discussing transparency in connection with the public-sector use of AI requires considering a twofold dimension of transparency: (i) external transparency, related to the disclosure of information about, e.g., AI-driven systems in the public sector, the bodies responsible for setting them up and managing them, the companies that have designed them or the award procedure; and (ii) internal transparency, related to the operation of the relevant AI solution, e.g., its scope of application or applicability, whether or not it is used for decision-making, the type of technology or the system's logical reasoning. External transparency has to do with transparency *stricto sensu*, i.e., with the obligation to disclose certain information on the grounds that it is relevant for citizens to understand how public authorities act.[53] Internal transparency has to do with the reasons or justification for the decisions adopted by or based on algorithmic systems, in order to show why the system does what it does.[54]

Based on these premises, bear in mind that transparency *stricto sensu* has a proactive and a reactive dimension. At this point, it is worth examining two provisions of the Charter of Digital Rights: XVIII and XXIII. Article XVIII refers to citizens' digital rights in their relationships with public authorities, and it includes two general requirements, which are not really novel, since they can be found in older statutory provisions. Firstly, it provides that the transparency principle applies to the digital environment. More specifically, Article XVIII secures the right of access to public information and seeks to guarantee compliance with active disclosure requirements. Secondly, Article XVIII requires that the public bodies responsible for any public action taken in the digital environment be identified. However, sections 6 and 7 do constitute a major development. These sections provide a general consideration and three specific safeguards directly related to transparency and the proper operation of any algorithms involved in administrative action or decision-making.

The general consideration is that citizens' AI-related rights under the Charter will be equally applicable within the context of administrative action. Article XXIII requires a human-centered approach and specifies that, in the development and life cycle of AI systems, the following rights must be secured: algorithmic non-discrimination; transparency, auditability, explainability and traceability; and accessibility, usability and reliability. On top of this, Article XXIII provides the right to request human supervision and intervention, and to challenge AI-based automated decisions having a personal or financial impact.

The specific safeguards–related to internal

[51] M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas)*, 77.

[52] F. Palmiotto Ettorre, *The Right to Contest Automated Decisions*, in *The Digital Constitutionalist*, available at https://digi-con.org.

[53] Royal Decree 203/2021, of 30 March, approving the E-government Regulation, provided for a significant twofold development in Art. 13 (although only applicable to national authorities, i.e., not to regional or local ones). On the one hand, the competent administrative body must issue a resolution authorizing a specific form of administrative action to become automated. On the other, such resolution must be posted on the body's website.

[54] G. Coglianese and D. Lehr differentiate between "fishbowl transparency" and "reasoned transparency." They consider that the first allows to understand *what* public authorities did and the latter explains *why* they took action. They are both connected: reasoned transparency depends on fishbowl transparency. After all, for the public authorities to offer a public explanation of why they took a specific action, they must, if nothing else, disclose what action they took. G. Coglianese and D. Lehr, *Transparency and algorithmic governance*, Faculty Scholarship at Penn Law, 2123, 2019, 9-15.

transparency–include (i) the right to receive an understandable reasoning expressed in natural language for the decisions adopted in the digital environment, backed by the relevant legal provisions, the technology used and the application criteria; (ii) a digital rights impact assessment of algorithm designs for automated or semi-automated decision-making; and (iii) that discretionary decision-making be reserved to persons. Finally, the Charter has incorporated the right to transparency regarding the use of AI instruments, including their operational structure and scope in each procedure, focusing on the data used, the margin of error, the scope of application and whether they are used for decision-making. Additionally, the Charter refers to the applicable legislation for the conditions to access the source code in order to verify that there are not any discriminatory outcomes.[55]

We welcome these provisions, due to their implications, but it is worth making two remarks. First, these are formal safeguards, which should be accompanied by an institutional guarantee, i.e., empowering a specific body to perform the prior verification and approval of algorithmic systems−whether one for each government level or a single body competent at all levels subject to a public-public arrangement. Second, they clearly show the Charter's weaknesses, since they are non-binding provisions. Public authorities may very well ignore any new developments if they are only provided in the Charter. In other words, these Charter provisions are mere guidelines. We are aware that the Charter was drafted as if it was eventually going to be a binding instrument, with the aim of inspiring and guiding upcoming rules. Precisely because of that, its entry into force will have a positive legal impact, since it will be applied by various legal actors–perhaps even judges will rely on it as interpretative guidance, or it may be incorporated into binding legal provisions. However, all of these positive impacts will depend on the legal stakeholders involved (judges, courts, governments and lawmakers), and not on the Charter's ultimate purpose. The law is not omnipotent. It needs policymaking to accomplish the ends pursued by legal provisions, but being a binding instrument is always key to achieve these goals. Unquestionably, the context does call for binding rules on the public-sector use of AI and algorithmic systems.

It is essential to set out a requirement for the legal feasibility of algorithmic systems: keeping track and documenting the initial programming method, the input data collected and selected, how the process worked, the trials, and any validations.[56] In particular, active disclosure duties should include any malfunctioning. This is all indispensable, not only from the perspective of transparency *stricto sensu*, but also, and more importantly, from the perspective of the duty to give reasons and oversight. In fact, being aware of these aspects (disclosure) is a pre-requirement for appropriately reviewing the legality thereof.

4.3. *Active disclosure and the right of access regarding public-sector use of AI*

As pointed out above, the Charter of Digital Rights provisions are not legally binding. However, a requirement for both external and internal transparency remains applicable to public authorities that exercise their powers by relying on algorithmic systems. In fact, both the LTBG and the LPAC include clear provisions that apply in this domain.

First, based on Art. 5(1) LTBG, one could argue that there is an active disclosure requirement covering algorithmic systems' operational structure, purpose, input data and actual functioning. Art. 5(1) LTBG requires public authorities to publish, on a regular basis, updated "*information that may be relevant to ensure the transparency of public authorities' activities related to the functioning and oversight of public action*." The use of algorithmic systems for administrative decision-making is most certainly relevant for these purposes. Therefore, all the information regarding its existence, applicability and scope must be made available on all the websites of public bodies relying on algorithms for decision-making.

Additionally, Art. 35 LPAC unambiguously establishes the duty to give reasons in any administrative acts that may

[55] These developments, or part thereof, were included in the proposal submitted by *Red DAIA* during the public consultation. See http://reddaia.org/ and the list of submitted proposals https://portal.mineco.gob.es/es.

[56] M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas)*, 78.

interfere with citizens' rights or interests.[57] Indeed, from a formal perspective, the use of algorithms neither excludes the duty to give reasons nor entails substantial changes as for the contents of the reasoning required in algorithm-driven administrative acts.[58] However, although there are requirements in place (which can be deemed applicable to the public-sector use of AI systems), it is advisable to strengthen the safeguards attached thereto. First, we must extend the transparency obligations related to model elaboration and system design,[59] adding to the list of active disclosure requirements under the general national legislation any information on the algorithmic system's technical specifications, input data, training results and eventual audits that have been performed, in order to prevent interpretations that are incompatible with the transparency principle. Second, reason-giving (although short) must be reasonable and tailored to the technology's distinct features.[60] On top of that, if any algorithmic prediction has a direct or indirect bearing on an administrative decision, it should be included in the reasoning, and the algorithm must be incorporated into the administrative file.[61]

Finally, we must assess if providing access to source codes is essential from the perspective of the duty to give reasons.[62] Self-evidently, accessing and evaluating the source code is the only way to know how the system operates from a technological perspective and, if appropriate, to detect any errors.[63] Also, the source code allows for verifying if the algorithmic system's programming is in line with the provision it applies or enforces.[64] In fact, some have claimed that there is a direct link between open source software–i.e., designing open source algorithms − and the principles of democracy and hierarchy in administrative organizations, since otherwise senior public officials (who are held accountable for the decisions) would depend on the code writers or programmers.[65] However, there are downsides to providing access to source codes, related to the possibility of "cheating" the system.

In Spain, this issue is already on the table from the perspective of the right of access to public information subject to transparency regulations. There is no point in examining all cases in depth, since that has already been done by legal scholars. Rather, we provide an overview of the approach to the matter.

The Transparency and Good Governance Council ruled on various appeals against decisions that denied requests to access the source code of certain computer applications. First, it is worth mentioning Resolution 701/2018, of 18 February 2019, stating that source codes qualify as public information, thus subject to the right of access, although in this specific case access was denied on

[57] On this matter, see E. Gamero Casado, *Compliance (o cumplimiento normativo) de desarrollos de Inteligencia Artificial para la toma de decisiones administrativas*, in *Diario La Ley*, No. 50, 2021, *in totum*.

[58] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Diritto dell'informazione e dell'informatica*, 2021, 440.

[59] J. Valero*, Las garantías jurídicas de la inteligencia artificial*, 88; along these lines, regarding the Italian system, see G. Pinotti*, Amministrazione digitale algorítmica e garanzie procedimentali*, in *Labour & Law Issues*, vol. 7, No. 1, 2021, 92.

[60] J. Valero, *Las garantías jurídicas de la inteligencia artificia*l, 88.

[61] A. Huergo Lora, *Administraciones Públicas e inteligencia artificial*, 89.

[62] J. De la Cueva, *La importancia del código fuente,* in F.S. Capilla Roncero (ed.), *Derecho digital: Retos y cuestiones actuales*, Cizur Menor, Thomson Reuters Aranzadi, 2019, 109-127; M.L. Gómez Jiménez, *Automatización procedimental y sesgo electrónico: el procedimiento administrativo electrónico desde la inteligencia artificial*, Cizur Menor, Aranzadi, 150, are in favor of allowing access to source codes. On the contrary, regarding non-predictive algorithms, Huergo Lora argues that, considering the currently applicable regulation, there is no need for (i) disclosing to citizens that a decision has been adopted through a computer application; or (ii) making the source code available (unless expressly required by a legal provision). However, regarding predictive algorithms–due to their innovative potential stemming from their ability to add self-elaborated content–he considers that public authorities should disclose the use thereof in decision-making. Huergo Lora argues that algorithms qualify as grounds of the administrative decision and thus must be incorporated into the file. See A. Huergo Lora, *Una aproximación a los algoritmos,* 72 and 85. Along these lines, G.M. Díaz González claims that disclosing source codes is not always the right answer, because (i) citizens lack sufficient knowledge to understand how the system works; and (ii) some systems are too complex for human understanding, aside from the fact that disclosure can negatively affect the very algorithm-driven administrative duty. See G.M. Díaz González, *Algoritmos y actuación policial: la policía predictiva*, in A. Huergo Lora (ed.), *La regulación de los algoritmos*, Cizur Menor, Thomson-Aranzadi, 2020, 189.

[63] D.K. Citron, *Open Code Governance,* 357.

[64] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, 441. According to this author, source codes should be (i) included in the reasoning, in the text, at least the part thereof that allows for verifying that the legal provisions and their translation into computer code match; and (ii) published or posted on the relevant public body's website.

[65] D.K. Citron, *Open Code Governance*, 358 ff.

intellectual property grounds, despite that the application (BOSCO, used by electricity marketers to determine if a given consumer qualifies as vulnerable and therefore is eligible for a discount) had been designed by the public administration.[66] More importantly, see Resolution 58/2021, of 20 May 2021, on a request to access the algorithm used to calculate social security pensions. The resolution reiterates that this algorithm qualifies as public information, and relevant information for that matter, since it explains how an administrative decision is made. Resolution 58/2021 adds a remarkable statement: "As long as there are no other mechanisms allowing to accomplish these transparency-related goals with equivalent guarantees–e.g., independent auditing or monitoring bodies–the only effective remedy is providing access to the algorithm, to its code, so it can be reviewed both by parties seeking redress for the algorithmic outcome and by citizens in general, for the sake of ethics and fairness." This statement has been replied in many other resolutions.

The first judgment in this matter delivered in Spain in the abovementioned BOSCO (electricity bill-related) case departed from this line of reasoning. Judgment of 30 December 2021 (proceedings 18/2019) issued by Central Judicial Administrative Court n. 8 takes a different approach. It upholds the aforesaid intellectual property grounds but, more importantly, it relies on the premise that "refusing access to the computer application's source code does not breach the legality principle, since, ultimately, it can be verified if the applicant is eligible for the discount tariff." Additionally, the Court holds that the app is a mere tool at the administrative body's service: "[T]he administrative act is not issued by a computer application, but by a public authority. The addressee may challenge the act through the relevant administrative appeals and judicial remedies. Thus, the legality of the administrative act is not backed up by the (ancillary) app used at a stage of the administrative procedure. Rather, the legality of the act is supported by the legal provisions on the subject-matter" (legal basis 3).

It is worth noting the intrinsic ties between external and internal transparency. Indeed, reason-giving can be affected by the limits on active disclosure as applied to the existence and use of algorithmic systems. A broad requirement to disclose information on the system's design, purpose, underlying functioning, input data, tested margin of error and accuracy or audit results enhances the reasoning of the algorithm-driven decision made by public authorities. However, despite the efforts made to deliver a duly reasoned decision in a specific case, the reasoning will hardly be acceptable in the absence of the above algorithm-related information when dealing with autonomous systems. Reasons are not enough; it is essential to know that the system is functioning correctly[67].

Keep in mind that reason-giving does not only have consequences for the specific case in which it is provided. Although it refers to individual procedures and to the particular decision made therein, decisions adopted *en bloc* on the basis of a programmed system could have an impact that goes beyond the specific case at hand.[68] Therefore, together with the safeguards provided for the parties concerned, we must secure guarantees seeking to protect all citizens.[69] Simply put, algorithmic systems' potential impact requires having the ability to verify their functioning, in accordance with the principles of transparency and participation.[70]

These considerations also apply from the perspective of administrative scrutiny and judicial-administrative review. Despite being unable to "enter" the decision-maker's mind, when dealing with algorithms we must learn

[66] The Catalonia Regional Commission for Guaranteeing the Right of Access had already ruled along these lines in joined Resolutions 123 and 124, of 21 September 2016, regarding access to an algorithm that determined the composition of the teacher boards for correcting university entrance exams. These resolutions require to disclose the algorithm to the applicant in mathematical language (if available) or, at least, in natural language, in order to allow the parties to learn how the system is run.

[67] See the complete analysis about the many questions relating to transparency in L. Cotino Hueso, *Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad...). Para qué, para quién y cuánta*, in L. Cotino Hueso and J. Castellanos Claramunt (eds.), *Transparencia y explicabilidad de la inteligencia artificial*, Valencia, Tirant lo Blanch, 2022, 25-70.

[68] G. Coglianese and D. Lehr thus claim that in most cases it will suffice to show that the system has been designed and is run to advance a legally valid purpose and that it is functioning correctly to advance that purpose in the case at hand. See *Transparency and algorithmic governance*, 40 and 47.

[69] G. Pinotti, *Amministrazione digitale algoritmica*, 85.

[70] D.K. Citron, *Open Code Governance*, 357.

how that "programmed mind" reasons, particularly if it operates with certain degree of autonomy.

In a nutshell: transparency and reason-giving are premises, requirements for monitoring compliance with the legality principle.[71] Applying the obligations arising from these premises at the algorithm design stage is a necessary modification.

However, transparency and reason-giving have further-reaching implications. These are not merely formal aspects. In fact, they have substantive dimensions[72] that could affect the merits or the very substance of administrative action. Consequently, failure to fulfill transparency and reason-giving obligations could render the decision invalid or voidable.

Finally, transparency and reasoning are also linked with a twofold technological element: explainability and interpretability.

On the one hand, explainability is associated with the internal logic and mechanics that are inside a machine learning system.[73] On the other, interpretability is mostly connected with the human intuition or understanding behind the outputs of a model, and it is an indispensable requirement if negative or unexpected outcomes could harm the parties concerned–therefore, it is not as important in cases in which the system is sufficiently tested and validated that we trust its decision, even if the system is not perfect.[74] So, an interpretable model is not always a model whose internal logic is understandable by humans.

This matter has a direct impact on the formal requirements applicable to algorithmic systems from the perspective of transparency and review. Interpretability does not always mean explainability and vice versa.[75]

Drawing this distinction is important because it aptly illustrates a claim that most scholars reject: transparency and reason-giving do not necessarily entail full openness of algorithmic systems in every single case. Transparency and the duty to give reasons relate to the system's legitimacy, and fulfilling this aim does not always require disclosing the system as a whole, i.e., the source code.[76] What really matters in legal terms is to disclose that the system exists, the input data, information about its technical operability and the reasons on which the decision is founded. Formal transparency and legal reasoning matter; the internal technical processes to arrive at a decision, not as much. In sum, there is a need for an explanation in ordinary language on the system's functioning logic, but not on its mathematical or computer logic. Legally speaking, the inner workings of an algorithm is not what is in need of explanation, but rather, the human interaction with the output of the algorithm and the criteria used in designing the inputs to safeguard the decision's understandability.[77]

For the sake of legal certainty, the principle of democracy and the right of defence, all of the above should come together in a statutory provision.

5. *Concluding remarks: some necessary safeguards*

Public-sector use of AI is not a given or an imposition. There is great latitude for deciding which issues should be solved, what is the most suitable solution and how we must implement it in each case. Disregarding AI altogether, thereby waiving the principle of effectiveness by failing to incorporate the best available technology and thus wasting its potential is not an option, but neither is blindly or uncritically applying AI systems as if there were no other options or approaches.

The key to identifying AI's role and scope in administrative law must always be the same: relying on technological innovations to

[71] In this regard, A. Soriano Arnanz considers that the lack of transparency of algorithmic systems makes it hard to review the legality of the software used for automated decision-making and hinders the parties' ability to challenge the outcomes. See A. Soriano Arnanz, *Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos*, in Revista *de Derecho Público: teoría y método*, No. 1 3, 2021, 94.

[72] E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Diritto Amministrativo*, No. 2, 2020, 293.

[73] P. Linardatos, V. Papastefanopoulos and S. Kotsiantis, *Expainable AI: a review of machine learning interpretability methods,* in *Entropy*, No. 23, 2021, 2-3.

[74] F. Doshi-Velaz and B. Kim, *Towards a rigorous science of interpretable machine learning,* available at https://arxiv.org/abs/1702.08608.

[75] P. Linardatos, V. Papastefanopoulos and S. Kotsiantis, *Expainable AI,* 3.

[76] H. Palmer Olsen, J. Livingston Slosser and T. Troels Hildebrandt, *What's in the Box? The Legal Requirement of Explainability in Computationally Aided Decision-Making in Public Administration*, in *iCourts Working Paper Series*, No. 162, 2019, 224.

[77] H. Palmer Olsen, J. Livingston Slosser and T. Troels Hildebrandt, *What's in the Box?*, 227.

solve legal issues. In other words, we need to make sure that AI is not merely compatible with the rule of law, but actually integrates its core principles.[78]

Admittedly, we still need a deeper knowledge about the power of AI, but it is safe to say that there is room for AI systems in administrative law, and specifically for self-learning algorithms. In a context of exponential increase in data, we need algorithms to manage all this information in order to improve decision-making processes.

The initial approach should be to take advantage of all available tools to optimize decision-making criteria. Accordingly, we can assert that the principle of sound administration−along with the duty to act and decide or adjudicate with due diligence when weighing all the facts, interests and rights at stake−requires to embrace the use of AI. Note that AI, and in particular algorithms, can effectively contribute to improving administrative action. For the moment, however, it is just a tool that transforms information into predictions that help us make decisions. I do not believe that that the full understanding of algorithmic reasoning by human operators is the core issue. Algorithmic opacity can turn into algorithmic transparency through appropriate design requirements.[79] However, we do need to identify a set of essential safeguards and legality criteria that allow to maintain a minimum degree of machine autonomy while preventing deviations and biases,[80] detecting vulnerabilities and correcting errors. Drawing clear boundaries is also a must. These boundaries must include excluding the application of AI from strictly and inherently human tasks. Ultimately, the key lies in the idea of human-machine cooperation and in how they complement each other: we need to use AI[81] in places that are off-limits for the human mind, always subject to human oversight and respecting the rights and safeguards of the parties affected by administrative action. Especially–and this should be the starting point–we must rely on AI for any tasks to which human capacity does not provide any added value, i.e., simple or routine tasks.

Therefore, it is essential to keep the actual risks in mind. Although this may not be the place to discuss biases in depth, note that an algorithmic bias occurs when a given system, due to faulty training data, methodology or model design, delivers different results based on the group to which the individuals belong, thus prejudicing them for belonging to that group.[82] However, keep in mind that what is generally considered a bias could be a natural consequence arising from the system's input data, where the system simply delivers a statistical reasoning with probabilistic outcomes. If data objectively lead to an outcome, there is no malfunctioning or bias, but simply an output from the data.[83] It would be necessary to carefully weigh and assess the actions and decisions to be taken on a case-by-case basis to prevent pattern categorization and identification from harming individuals who, despite being a match, do not meet the conditions for being subject to the applicable legal rule.

This calls for a deeper reflection to answer two questions: given the large amount of available data, is it feasible or realistic to implement major transformative AI-driven projects? Would it be better to focus on enhancing data quality or establishing parameters aimed at ensuring the quality of data in the future? In sum, although there will always be bias-related risks, in order to face this challenge we must plan and regulate data governance.[84]

[78] M. Hildebrandt, *Algorithmic regulation and the rule of law,* in *Philosophical transactions*, Series A, Mathematical, Physical, and Engineering Sciences, 2018, 9.

[79] C. Coglianese and D. Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, in *Georgetown Law Journal*, 2017, 7.

[80] C. Campos Acuña, *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*, No. 3, 2019, 87, available at www.ivap.euskadi.eus.

[81] This statement can be backed up by the following fact provided by D. Cardon: if we scanned all communications and papers written from the beginning of time until 2003 to store them, we would need 5 billion gigabytes. Currently, it takes two days to generate this amount of data or information: D. Cardon, *Con qué sueñan los algoritmos*, 18.

[82] M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas)*, 53.

[83] On this issue, M.L. Gómez Jiménez points out that if we cannot eliminate these biases by appropriately re-programming the system, any acts based on such system should be invalidated, M.L. Gómez Jiménez, *Automatización procedimental y sesgo electrónico*, 149. In my opinion, this would not always be the case.

[84] See a thorough analysis on preventing algorithmic discrimination in A. Soriano Arnanz, *Data protection for the prevention of algorithmic discrimination*, Cizur

There is a general need for safeguards and principles. The ones in place right now meet our needs for the most part, but sometimes, regarding specific aspects, they may need an appropriate *ad hoc* response tailored to the reality of AI. E-government does not only consist in incorporating technological tools into the grids of administrative law, but it also entails a revision of the parameters for framing reality. Nevertheless, the general doctrinal categories remain useful. The principle of transparency, the principle of disclosure, the principle of sound administration, the principle of legality, the principle of accountability are general categories that, maybe with new nuances, are still valid and relevant in the field of administrative law. Likewise, the categories of defects of administrative decisions can be applied to the grounds for invalidity: material errors, unreasonableness of the solution chosen by the system, abuse of power in programming, inadequate statement of reasons, or lack of competence.

There is, however, a big difference: public authorities can decide through non-human intelligence; i.e., self-learning algorithms that can handle information and make decisions based on knowledge that humans cannot obtain by themselves. As legal scholars and technology experts, we should focus our efforts on this aspect.

So, while preserving the general categories, their specific application to automated administrative activity will have to be adapted in certain instances. The following proposals seek to strike a balance between technology and law—ultimately, to "humanize the machine."[85]

All of these proposals are premised on the following key aspects, which also aptly summarize the above insights. These key elements must provide the foundations for rethinking and, if appropriate, rebuilding, new principles or new safeguards: (i) human primacy and human control over algorithmic systems; (ii) transparency and explainability; (iii) prior approval of the systems based on risk assessment; (iv) system functioning auditability; and, always (v) available legal remedies to challenge any actions or decisions.

Human control or oversight over algorithms suggests that algorithms be subject to constant monitoring. The need for the prior approval of algorithmic systems is justified because we need to (i) detect any issues to be tackled within the organization through AI-driven tools and techniques; (ii) pick the most suitable instrument; and (iii) implement the AI solutions with appropriate legal and technological safeguards. Since algorithms pre-determine final acts or decisions, they must be directly challengeable.

Moreover, see below three specific proposals, which would require regulation, that aptly summarize this paper.

First.- Shaping a new principle: the "principle of minimal automated activity." There is no doubt about the applicability and effectiveness of the general principles of law in our system. They reflect or represent social values and thus guide other sources of law or legal instruments, helping to interpret them all and applying by default.[86] The use of big data, and in particular personal data processing, entails significant risks; for instance, the lack of knowledge of the data used by the algorithms or the inability to fully understand the rationale underlying the final prediction-decision. This reinforces the idea that automated administrative action based on machine learning should be (at least for the moment) limited to factual or formal actions with no political discretion involved. Also, the head of the administrative body using the machine should in any case remain materially and formally accountable. In areas where there is certain political discretion, the machine's role will be to support decision-making, but not to replace it.[87] Considering

Menor, Thomson Reuters-Aranzadi, 2021.

[85] V. Frosini, *Cibernética, Derecho, Internet y Sociedad*, 70.

[86] L. Ortega Álvarez, *Funcionalidad y eficacia de los principios generales del Derecho*, in *Justicia Administrativa*, No. 15, 2002, 5-22.

[87] D. Marongiu considers that human control of the results produced by the machine in the exercise of authority must be absolute and permanent, and he concludes that AI should only be used in the field of administrative activity regarding public services: D. Marongiu, *Inteligencia artificial y administración pública,* in C. García Novoa and D. Santiago Iglesias (eds.), *4ª Revolución Industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*, Cizur Menor, Thomson-Aranzadi, 2018, 396-397. According to M. D'Angelosante, the indeterminate nature of the criteria to be ascertained and evaluated prior to the decision, and the decision's discretionary nature, represent obstacles for automation: M. D'Angelosante, *La consistenza del modello dell'amministrazione "invisibile" nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le*

technology's current development, there is no room for automated, algorithmic-driven discretionary powers, precisely because of this "political" scope of action. The expression of political-administrative will, which entails direction, coordination or similar action, must be human.[88] However, this does not preclude the competent authority from relying on AI systems to make the decision.

At present, human intervention cannot be suppressed altogether,[89] since machine learning is predictive in nature and does not allow for causal interpretation.[90] Ultimately, algorithmic systems must be used if there is room for improving public authorities' action,[91] not only from the perspective of effectiveness and efficiency, but also with the aim of fulfilling citizens' rights.

It is of paramount importance to ensure data quality. If this premise is not fulfilled, the principle of data quality will remain applicable and there would be no room for using algorithmic systems for administrative decision-making.[92]

So, using an algorithm will only be allowed if (i) the aim pursued can be accurately and clearly determined; (ii) there is sufficient quality data to take action; (iii) and the algorithmic system has been successfully tested, considering its potential risks for citizens' rights and interests, and citizens have had the opportunity to get involved in the algorithm's design and set up.[93] On top of that, keep in mind that using algorithms will only be possible for highly structured and parametrical areas of decision-making, where abstract concepts do not prevail, since they are hard to codify.

Second.- Specifically regulating the process of adoption of computer programs and the transparency of their operation. Such regulation must fulfill and reinforce the general principle of transparency and the principle of impartiality regarding the system configuration and the implementation thereof. Although these principles are currently applicable, there must be specific rules to enforce them regarding the use of algorithms. For instance, participation requirements must apply both to system design[94] and to the system's implementation, allowing the parties concerned to have an impact on the final algorithmic-driven decision. The dehumanization inherent to automated decision-making should not deprive citizens of a human reference to raise concerns or objections, aside from any legal remedies at their disposal to challenge the decisions. Also, it is vital to ensure (i) the objectivity of the data used; and (ii) the impartiality of the transformation of data into predictions or forecasts. A new regulation on algorithm

decisioni, in S. Civitarese Matteucci (ed.), *A 150 anni dall'unificazione amministrativa italiana – La tecnificazione*, Firenze, Firenze University Press, 2016, 166.

[88] B. Raganelli, *Le decisioni pubbliche al vaglio degli algoritmi,* in *Scritti in onore di Eugenio Picozza*. Naples, Editoriale scientifica, 2020, 15. She puts forward three forms of interaction or dialogue between AI and discretionary decision-making: (i) preclusive dialogue, where there would be no room for algorithms because there is extensive discretion; (ii) cooperation-based dialogue, under which AI is a useful tool to support discretionary decisions; and (iii) self-regulated dialogue, in which AI is used to limit the exercise of discretionary powers by pre-defining future action and becoming bound to its own rules. (18 ff.).

[89] J. Ponce Solé argues that the use of AI in fields of discretionary decision-making should be precluded. He advocates to regulate a "reserve of humanity" or an "only-human-decision-making clause" to ensure that certain decisions can only be taken by humans: J. Ponce Solé, *Inteligencia artificial, Derecho administrativo y reserva de humanidad,* 26-33. A. Cerrillo claims that we must acknowledge the need to ensure human supervision in the use of algorithms to prevent negative effects. Human oversight could entail incorporating into discretionary decision-making a mechanism for human intervention, where humans could review or validate the decision taken by the machine. See A. Cerrillo, *El impacto de la inteligencia artificial en las Administraciones Públicas,* 82. Along these lines, M. Moreno Rebato holds that using high-risk AI systems requires human oversight; M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas),* 53. M. D'Angelosante, imagines a scenario where machines operate autonomously, and public officials only intervene in the decision-making process in the event of disputes over the choice made by the machine: M. D'Angelosante*, La consistenza del modello dell'amministrazione "invisibile*", 157. She also considers that replacing public officials would impinge on citizens' right to a personalized interlocutor (p. 161).

[90] C. Coglianese and D. Lehr*, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 23-24.

[91] C. Coglianese and D. Lehr, *Transparency and algorithmic governance*, 55-56.

[92] E. Carloni insists on the idea that the legality or lawfulness of administrative action is not only secured by the algorithm's understandability, the ability to challenge it and monitor it, and a public official's validation. Also, it will be necessary to make sure that the system does not incur in discrimination. To that end, proving data quality is a requirement. See E. Carloni, *I principi della legalità algoritmica,* 289.

[93] C. Coglianese and A. Lai, *Algorithm vs. algorithm,* 1324-1337.

[94] G. Pinotti, *Amministrazione digitale algoritmica e garanzie procedimentali*, 89.

openness is required:[95] there is a need to disclose the values of the source code both in mathematical terms and as purposes, which are configured as conditions of legitimacy. In short, the decision to use algorithms in the context of an administrative procedure or for the development of an administrative activity must be public. Therefore, we need to implement a prior approval process for these systems.[96]

The focus should not only be on why the decision was adopted, but also on the decision-making process.

Third.- Creating a specialized, independent oversight body. In the exercise of their supervisory functions, these specialized administrative bodies would be responsible for approving the algorithmic codes and their specific operational structure, as well as for ensuring proper functioning during the algorithm's life cycle.[97] Article 41 LRJSP (currently in place) requires that the body or bodies competent for monitoring algorithmic quality and, if appropriate, auditing the system and its source code, be determined prior to taking automated administrative action. Therefore, this provision is indirectly requiring that these duties be performed in practice.[98] However, specialization is key in AI-related matters. These specialized bodies would support the judicial review performed by judicial-administrative courts. The paradigm shift brought by algorithms has a major implication: scrutiny and oversight must focus on programming and not only on decision-making.[99]

Although using different names–deterministic and non-deterministic, conditional and non-conditional, or code-driven and data-driven algorithms–a distinction is often made between algorithms that faithfully follow pre-existing programming patterns and algorithms that learn from input data. In any event, from a legal perspective, it is essential to focus on a twofold aspect: (i) how the legal provisions enforced by algorithms (whether by

[95] K. Miller holds that legitimacy and reasonableness of algorithm-based decisions depend on the transparency of the decision-making system: K. Miller, *The application of Administrative Law Principles to technology-assisted decision-making,* in *AIAL Forum*, 86, 2016, 31.

[96] Its practical value can be better seen in specific cases. It is worth examining the use by the Andalusian Regional Government of a robotic automation solution for awarding thousands of subsidies to self-employed workers under Regional Decree 622/2019, of 27 December, on E-government. Together with the safeguards of Article 41 LRJSP, Article 40 of the regional decree requires the need for the prior approval of any activities subject to automated administrative decision-making. See a critical view in E. Benítez Palma, *La transformación digital del control externo del gasto público,* in *Auditoría Pública,* No. 76, 2020, 19-30, available at https://asocex.es.

J. Valero is one of the greatest advocates of prior approval processes for AI systems in Spain. Based on Art. 41 LRJSP, he considers that prior approval is an essential pre-requirement for appropriately protecting citizens' rights and interests. He is also in favor of establishing autonomous *ad hoc* boards to hear any appeals against (i) AI-driven administrative acts; and (ii) the implementation of algorithmic systems. See J. Valero, *Las garantías jurídicas de la inteligencia artificial,* 87 and 91. In the same vain, derived from the consideration that the algorithms are regulations, A. Boix, *Algorithms as Regulations: Considering Algorithms, when Used by the Public Administration for Decision-making, as Legal Norms in order to Guarantee the proper adoption of Administrative Decisions*, in *European Review of Digital Administration & Law* – Erdal, 2020, Vol. 1, Issue 1-2, 75-99.

E. Carloni holds that the administrative *lex certa* principle governs fully automated processes, thus only requiring a prior enabling provision. Conversely, he claims that for semi-automated processes it would suffice to apply the general principles of autonomy and organizational discretion. See E. Carloni, *I principi della legalità algoritmica,* 295.

A.G. Orofino argues that the adoption of the programing rules must be formalized in an administrative act: A.G. Orofino, *La automazione amministrativa: imputazione e responsabilità,* in *Giornale di diritto Amministrativo*, 2005, 1308-1309.

[97] A. Cerrillo has advocated for creating independent oversight agencies to monitor the algorithms used by public authorities. These agencies could be supported or assisted by auditing entities. See A. Cerrillo, *El impacto de la inteligencia artificial en el Derecho Administrativo,* 2019, 27. M. Moreno Rebato agrees. See M. Moreno Rebato, *Inteligencia Artificial (Umbrales éticos, Derecho y Administraciones Públicas),* 81. He argues that such an independent oversight entity could be tasked with assessing compliance with the established technical and legal requirements and the impact on citizens' rights, by examining the system's source code, the data and other documents.

[98] E. Gamero Casado, *Compliance (o cumplimiento normativo) de desarrollos de Inteligencia Artificial para la toma de decisiones administrativas*, in *Diario La Ley*, No. 50, 2021, 3.

J. Ponce considers algorithm audits a feasible alternative in cases where full disclose–access to the source code–is impossible or not advisable: J. Ponce, *Inteligencia artificial, Derecho administrativo y reserva de humanidad,* 46. G. Vestri claims that these auditing and oversight duties be conducted by private companies independently and confidentially. See G. Vestri, *La inteligencia artificial ante el desafío de la transparencia algorítmica,* in *Revista Aragonesa de Administración Pública*, No. 56, 2021, 391.

[99] M.L. Gómez Jiménez, *Automatización procedimental y sesgo electrónico*, 140.

supporting a decision or making the decision altogether) have been translated into computer code; and (ii) the input data used by the system to operate and to accomplish its design objective. Accordingly, there should be two ways of challenging an algorithmic-driven decision: (i) a direct appeal against the adopted decision on the grounds that it is unlawful; and (ii) an indirect appeal, based on (a) a misinterpretation of the applicable legal provisions at the time of designing the system; or (b) faulty input data or defective training.[100]

Certification of an AI system's transparency, accountability and fairness[101] can help in accomplishing this objective. Appointing persons within an organization responsible for ensuring regulatory compliance in the design and use of AI systems is also necessary. Additionally, it can be helpful to establish a register of the algorithms and AI systems used by public authorities,[102] as a tool to promote transparency vis-à-vis citizens regarding the existence thereof. However, lacking a direct link with citizens, these safeguards do not suffice from the perspective of the legitimacy of administrative action. So, in addition to assessment and certification bodies and systems we need to implement appropriate accountability mechanisms.[103]

In simple terms, insofar as algorithmic-driven decisions can be explained by the way algorithms have been programmed and enforce rules, we need to be aware and assess these aspects in order to control such algorithmic decision-making.[104]

On top of that, it is key to rethink human resource selection, organization and management.[105] Public authorities can no longer be "enslaved" to the private sector regarding the use of technology. This does not mean that all technological developments within an administrative sphere must be public. Indeed, private sector cooperation and partnership is indispensable, but we do need to advance public authorities' capacity to create public algorithms.

Finally, ethics should be at the center of the debate and the analysis regarding the use of algorithms and algorithmic system programming, although never *in lieu* of the law.

So, before embracing smart administration (i.e., smart government) as the new paradigm of administrative law, we must further examine the notion of rational government, i.e., "irrationality-less" public authorities that act rationally because they rely on algorithms and appropriately manage big data, thus being able to make sounder and more logical decisions.

Public authorities apply and enforce the law based on the information and technology at their disposal. Automation and AI provide access to a larger amount of information, and they allow for better data processing. Consequently, automation and AI exceed human knowledge-generating abilities. Law cannot be reduced to the much more restricted circle of rationality,[106] although operational rationality applied to administrative organization and procedure can render administrative action more effective and objective.[107] Algorithms are not, by themselves, a source of authority. Rather, they are instruments at public authorities' service. Us human beings are more than data. An administration will never be "intelligent" if it fails to fulfill the relevant principles and safeguards. This is the key to striking the right

[100] M. Hildebrandt, *Algorithmic regulation and the rule of law*, 3.
[101] See *Ethics Guidelines for Trustworthy AI*, 28.
[102] This claim is made by A. Soriano Arnanz, *Decisiones automatizadas: problemas y soluciones jurídicas,* 115; and O. Cortés, who also argues that periodic inspections would be necessary to verify the operation of any registered algorithms: O. Cortés, *Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración Pública*, in *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, No. 18, 2020, 59.
[103] J.A. Pinto Fontanillo, *El Derecho ante los retos de la Inteligencia Artificial. Marco ético y jurídico*, Madrid, Edisofer, 2020, 91.
[104] J. Cobbe, *Administrative Law and the Machines of Government*, 8.
[105] On this topic, see a comprehensive approach in R. Galindo Galdés, *Automatización, inteligencia artificial y empleados públicos,* in *Retos jurídicos de la inteligencia artificial,* A. Cerrillo i Martínez and M. Peguera Poch. Cizur Menor, Thomson-Reuters Aranzadi, 2020, 93 ff. From the perspective of political science, C. Ramió, *Inteligencia Artificial y Administración Pública*, *in totum*, has very interesting insights.
[106] V. Frosini, *Cibernética, Derecho, Internet y Sociedad*, 38.
[107] S. Barona Vilar contends that technological devices have given way to a new life ideology that is directly connected with the control of individuals and that therefore calls for major efforts to preserve the pre-existing values and human rights, which are at risk of being seized or voluntarily surrendered. See S. Barona Vilar, *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Valencia, Tirant lo Blanch, 2021, 17.

balance between algorithms and administrative action. Right now, a pre-condition for this balance is to use algorithmic systems to collect information relying on data and subsequently making it available to human decision-makers. Thus, within the public sector, it is for humans to implement the transition from mere computation to decisions with an impact on the real world.

The history of administrative law is a struggle between power and freedom.[108] When it comes to technology, and AI in particular, we broaden the boundaries of knowledge, but that does not necessarily entail that we loosen the boundaries of freedom.[109] Striking a fair balance requires to review categories, legal institutions, concepts and contexts. Then, we must carefully and appropriately assess the potential clashes between (i) the new challenges posed by the public-sector use of AI; and (ii) citizens' principles and rights. That was–with a limited scope–the ultimate aim of this paper.

[108] E. García de Enterría, *La lucha contra las inmunidades del poder en el Derecho Administrativo (poderes discrecionales, poderes de Gobierno, poderes normativos)*, in *Revista de Administración Pública*, No. 38, 1962, 159-208.
[109] J.M. Lasalle, *Ciberleviatán*, 78.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 31-44
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 03

*Law, Digital Nudging and Manipulation: Dark Patterns, Artificial Intelligence and the Right to Good Administration**

Juli Ponce
(Full Professor of Administrative Law at the University of Barcelona)

ABSTRACT The use of behavioural insights in the digital area has grown considerably in importance during the COVID-19 pandemic and can be an element of promoting the right to good administration in the public sector. On the other hand, digital nudging has a dark side, both in private and public sector. The possible use by public and private sectors of so-called dark patterns, concerning which the European Parliament has recently proposed to include a ban in the future Digital Services Act, and what is known as hypernudging raises legal questions regarding a possible manipulation that violates freedom of thought, as indicated by the Committee of Ministers of the Council of Europe in a statement of 2019. This article deals with the definition of those concepts and their possible legal regulation, by means of considering some international examples.

1. *Introduction*

The Covid-19 pandemic has led to a dramatic rise in Internet use. Recent research shows, in fact, that in the past year there has been an increase of up to 30% in digital consumption.[1]

In this digital environment, choice architectures are constantly made, either actively or passively. For those who are not familiar with the term, choice architecture is a concept reflecting the awareness that the choice between different options is affected by the way in which such options have been proposed.[2]

Humans face choices every day, but the result of every decision is influenced not only by rational deliberations regarding the available options. The design of the choice environment in which the information is presented can exert a subconscious influence on the outcome. In other words, the decision often depends on how the choice is presented; hence, decision architecture alters people's behaviour in predictable ways. The simplest changes in the choice environment —in which options are presented— can influence people's decision and "nudge" them to behave in certain ways. In fact, there is no neutral way to present options. For example, it has been proven that the mere act of changing the default options for organ donation —from opt-in to opt-out— has almost doubled the percentage of people who consent to donate organs.

There is always a design of the context of decision, which is created and modelled —consciously or unconsciously— by an architect of the choice: a context in which consumers and users of public services choose between specific options and come to decisions (buying, getting vaccinated, etc.) and the same happens in the digital ambit.

Accordingly, it is inferable that there can be —and there actually are— private and public activities aimed at encouraging or discouraging consumers and users' behaviour both outside and —most importantly— within the digital world. These architectures of choice can be transparent or not and have purposes that may turn out to be acceptable and even positive (e.g. encouraging consumption without scams, respecting the will of the consumers, customizing public services to provide better public management, etc.) or ethically and legally unacceptable[3] (e.g. increasing the sale of products or services to consumers, guiding or hindering the use of public services,[4] obtaining personal

---

* Article submitted to double-blind peer review.
This article is one of the results of the Spanish National Project PID2020-115774RB-I00, Citizen-Centric Services, Biases and Artificial Intelligence: Towards a Consolidation of Digital Rights in Public Administrations, funded by mcin/aei/10.13039/501100011033.

[1] See figures provided by WARC: *Data Global Ad Trends: The State of the Industry 2020/21*, in www.warc.com

[2] R. H. Thaler, C.R. Sunstein and J.P. Balz, *Choice architecture,* in E. Shafir (ed.), *The behavioral foundations of public policy*, Princeton, N.J., Princeton University Press, 2013, 428.

[3] M. Lavi, Evil nudges, in Vanderbilt Journal of Entertainment & Technology Law, vol. 21, issue 1, 2018, 1.

[4] R.H. Thaler, *Nudge, not sludge*, in *Science*, vol. 361, issue 6401, 2018, 431.

data without a clear and explicit consent —thus manipulating people—, etc.).

In other words, in those and other cases, we are dealing with digital nudges. A nudge is, according to Thaler and Sunstein's well-known definition, any cheap and easy-to-avoid aspect of the architecture of decisions in the digital environment that modifies people's behaviour in a predictable way, without prohibiting any option and without changing economic incentives.[5] Therefore, digital nudging, for the purpose of this reflection, is the use of user interface design elements to guide people's behaviour in digital choice environments. In turn, digital choice environments are user interfaces —such as web forms and ERP (Enterprise Resource Planning) screens— that require people to make judgments or decisions.[6]

Given the current spectacular growth in the use of digital media, the architecture of digital choice is gaining importance and the same happens in the case of the digital incentives or nudges that persuade consumers and users of public services.

The present article is a brief analysis on how these incentives are developing in the private and public sectors. It will address the possible use, by governments, digital platforms and companies, of behavioural insights achieved in recent decades. In the case of public sector, those digital incentives can be a way of promoting the right of good administration (art. 41 of the European Charter of Fundamental Rights and equivalent national regulations[7]), but their digital application can be also used to take advantage of people's cognitive biases with the consequent risk of inacceptable manipulation —specifically identified by the Committee of Ministers of the Council of Europe in the *Declaration on the manipulative capabilities of algorithmic processes* of 13th February 2019.[8]

It is important to highlight that a recent publication promoted by the Council of Europe warned: "Special attention should also be paid to the potential use of AI in human-machine interaction to implement nudging strategies. Here, due to the complexity and obscurity of the technical solutions adopted, AI can increase the passive role of citizens and negatively affect the democratic decision-making process. Otherwise, an active approach based on conscious and active participation in community goals should be preferred and better managed by AI participation tools. Where adopted, nudging strategies should still follow an evidence-based approach".[9]

2. *The dark side*

Going to our first ambit of analysis, applications and websites in the private sector —without specific regard to AI —, it is necessary to reflect, first of all, on the expression that designates the manipulative use of digital nudges to the detriment of consumers and users: dark patterns.

The article will subsequently endeavour to answer some essential questions regarding dark patterns:

- What are dark patterns?
- Which are the most common dark patterns?
- What cognitive biases do dark patterns exploit?
- What can be done against them?
- Should public intervention be necessary against dark patterns? Which type of intervention?
- Is there any other open issue regarding dark patterns?

2.1. *What are dark patterns?*

According to the insights of various specialists,[10] dark patterns are designs of User Interface (UI) and User Experiences (UX) that try to exploit people's vulnerabilities through manipulation and scamming with the intention of pushing them towards a certain outcome.

This definition highlights the breadth of the concept of dark patterns as well as the vast number of purposes they can serve (e.g., obtaining more personal data, money, influencing a vote or, in general, any decision).

[5] R.H. Thaler and C.R. Sunstein, *Nudge. The Final Edition*, London, Penguin Books, 2021.
[6] M. Weinmann, C. Schneider and J. vom Brocke, *Digital Nudging*, in *Business & Information Systems Engineering*, vol. 58, issue 6, 2016, 433.
[7] J. Ponce, The Right to Good Administration and the role of Administrative Law in promoting good government, in A. Cerrillo and J. Ponce (eds.), Preventing Corruption and Promoting good Government and Public Integrity, Bruxelles, Bruylant, 2017, 25.
[8] See Declaration by The Committee of Ministers on the manipulative capabilities of algorithmic processes, in www.coe.int.
[9] Council of Europe, Towards regulation of AI systems, 2020.
[10] See *Dark Patterns,* in www.darkpatterns.org.

Similarly, the *California Privacy Rights Act* (CPRA) of 2020, which, as will be explained, was recently amended to ban dark patterns, reports: "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation".[11]

2.2. *Which are the most common dark patterns?*

Dark patterns have been detected, studied and labelled with names that are undoubtedly original. Some concrete examples of these obscure designs, extracted from various sources will be presented hereafter to better understand the phenomenon.[12]

Confirmshaming. "Confirmshaming" is a dark pattern in which the user must choose between activating specific options/signing up for some service or not. In case of dissent, the consumer is made to feel bad, guilty or ashamed.[13]

Disguised Ads. This is a dark pattern in which ads appear "disguised", confused in the midst of normal content, video players or navigation elements, in order to mislead the user into clicking on them without noticing it.[14]

Forced Continuity. "Forced continuity" occurs when money is charged without warning at the end of a free trial of a service or in the case of subscriptions that are automatically renewed without asking for explicit consent.[15]

Friend Spam. The platform asks for permissions to access email, phone and/or social networks' contacts for a specific action —for example finding friends— but such permissions are used to send spam to the user's contacts.[16]

A few years ago, LinkedIn, which regularly resorted to this design was given a 13-million-dollar fine, as it was considered a clearly abusive practice.[17]

Misdirection. As suggested by the name, "misdirection" is a dark pattern consisting of a distraction of users aimed at making them follow a path that leads to a pre-set outcome and not to the one they really wanted to achieve.[18]

Price comparison prevention. This dark pattern hinders the comparison between one item and another in order to prevent users from making informed decisions.[19]

Privacy Zuckering. The name of this design combines —for obvious and well-known reasons— the surname of Mark Zuckerberg, Facebook's CEO, with the informal term "sucker". In fact, it takes place when users are tricked into sharing more private information than they really want. This is because the small print hidden in the terms and conditions that users accept in order to access online services gives permission to sell their personal data to other companies.[20]

Roach motel. Behind this name hides a very common practice that consists of facilitating the entry or subscription to a service and then making cancellation extremely difficult.[21]

Bait and switch. A dark pattern arising in those cases in which the user wants to realize an operation, but performs a completely different one, which is the one that interests the "misleading" website.[22]

Sneak into basket. This is an online sales systems' practice in which some extra items are included in the shopping basket to make people inadvertently buy them. Extra items are usually added via a checkbox or a radio button that is hardly visible during one or more steps of the purchase. It has been a very common practice on the websites of low-cost airlines.[23]

Hidden Costs. This dark pattern is very similar to the previous one, as it consists of the sudden inclusion of some extra costs, such

[11] See California Privacy Rights Act (CPRA) of 2020.
[12] C. Álvarez, Dark Patterns: the dark side of the UX, in www.wildwildweb.es; Dark Data — Zines, in www.parsons.edu.; Dark patterns - Types of dark pattern, in www.darkpatterns.org.
[13] See examples at *confirmshaming*, in www.tumblr.com.
[14] See example at *confirmshaming*, in www.tumblr.com.
[15] See examples at *Forced continuity - a type of dark pattern*, in www.darkpatterns.org.
[16] See examples at Forced continuity - a type of dark pattern.
[17] See After Lawsuit Settlement, LinkedIn's Dishonest Design Is Now A $13 Mil, in www.fastcompany.com.
[18] An example of this hard-to-define design can be found at *Misdirection*, in www.darkpatterns.org.
[19] See examples at Price comparison prevention - a type of dark pattern, in www.darkpatterns.org.
[20] See examples at Price comparison prevention - a type of dark pattern.
[21] See examples at *Roach motel - a type of dark pattern*, in www.darkpatterns.org.
[22] See examples at *Bait and switch - a type of dark pattern*, in www.darkpatterns.org.
[23] See examples at Bait and switch - a type of dark pattern.

as delivery costs or taxes. The main difference is that this one appears at the end of the sale process.[24]

2.3. *What cognitive biases do dark patterns exploit to manipulate consumers?*

The aforementioned examples of dark patterns seek to use consumer biases in a dishonest way to induce people to make mistakes/operations —or prevent them from doing specific actions— by manipulating them.[25]

Before going into the question in greater depth, it could be useful to say some words about cognitive biases.

In recent decades, thanks to the well-known work of the Israeli psychologists Amos Tversky —died in 1996— and the 2002 Nobel laureate Daniel Kahneman, psychology has contributed most to make it widely accepted that:[26]

- The absolute rationality of the person, of the *homo economicus* does not exist. First of all, because rationality is limited (as highlighted by Herbert Simon a long time ago) and, secondly, because it is a concept that does not take into account perfectly rational behaviors such as reciprocity and altruism (which give rise to a model of *homo reciprocans* that makes decisions based on social norms, in which reciprocity, altruism and trust matter).
- Rationality is interfered with by *heuristics* and *cognitive biases.* The works of the authors cited above point out that cognitive schemes and heuristics are rules that simplify the selection and processing of information. These are like intuitive *shortcuts*, which function as adaptive mechanisms against the limits of our cognitive resources (so a red octagon generally means "stop", while an outstretched hand expresses "greeting") and, in situations of risk and uncertainty, lead to certain assessment and prediction biases. Heuristics can provide fast and efficient shortcuts in information processing, but sometimes they also lead to systematic and predictable errors. Thus, heuristics produce errors, and biases are errors that occur systematically. Nevertheless, not all errors are biases, even though all biases are errors.

Due to these biases, *it is not unusual for our brains to mislead and* turn us into individuals who make mistakes and bad decisions, even when we have complete information. Although it may come as a surprise, since the deviations of people's rationality have already been studied well, the scientific advances of the last decades show us that people are not perfect decision-makers who maximize their interest in an absolutely rational way. Kahneman explained very educationally that two systems of decision-making coexist inside us: one is automatic and fast, the so-called system 1; while the other, system 2, is an effort linked to previous deliberation. System 1 is activated unconsciously and works well on various occasions, but on many others it leads to cognitive errors caused by those heuristics and biases that are used by our mind to make quick decisions without excessive energy consumption.

The main premise of the theory of cognitive psychology, therefore, is understanding that the human brain is a limited processor of information unable to successfully process all incoming stimuli.

Dark patterns are thus made to exploit cognitive biases; to affect humans and consumers' decision-making and emotions to their detriment and to the advantage of private companies that act as architects of people's choice.

"Confirmshaming", for example, exploits framing bias and sense of guilt, while "misdirection" takes advantage of lack of attention, the anchoring effect and scarcity bias, and so on... Some recent studies have already linked dark patterns with the cognitive biases that manipulate people to the advantage of companies.[27]

An overview of these connections can be found in the following table:

[24] See examples at *Hidden costs*, in www.darkpatterns.org.

[25] Those designs proved to be so significant that a member of the editorial board of the *New York Times* dedicated an article to them, available at: *Opinion | The Internet's 'Dark Patterns' Need to Be Regulated - The New York Times*, in www.nytimes.com.

[26] D. Kahneman, *Thinking, fast and slow*, Penguin Books, London, 2011.

[27] See A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty and A. Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites,* in CSCW, Article 81, 2019.

Legend: ●= Always, ◐= Sometimes, ○= Never

Category	Type	Description	# Instances	# Websites	Asymmetric?	Covert?	Deceptive?	Hides Info?	Restrictive?	Cognitive Biases
Sneaking	Sneak into Basket	Adding additional products to users' shopping carts without their consent	7	7	○	○	◐	●	○	Default Effect
	Hidden Costs	Revealing previously undisclosed charges to users right before they make a purchase	5	5	○	○	◐	●	○	Sunk Cost Fallacy
	Hidden Subscription	Charging users a recurring fee under the pretense of a one-time fee or a free trial	14	13	○	○	◐	●	○	None
Urgency	Countdown Timer	Indicating to users that a deal or discount will expire using a counting-down timer	393	361	○	◐	◐	○	○	Scarcity Bias
	Limited-time Message	Indicating to users that a deal or sale will expire will expire soon without specifying a deadline	88	84	○	◐	○	●	○	Scarcity Bias
Misdirection	Confirmshaming	Using language and emotion (shame) to steer users away from making a certain choice	169	164	●	○	○	○	○	Framing Effect
	Visual Interference	Using style and visual presentation to steer users to or away from certain choices	25	24	◐	●	◐	○	○	Anchoring & Framing Effect
	Trick Questions	Using confusing language to steer users into making certain choices	9	9	●	●	○	○	○	Default & Framing Effect
	Pressured Selling	Pre-selecting more expensive variations of a product, or pressuring the user to accept the more expensive variations of a product and related products	67	62	◐	◐	○	○	○	Anchoring & Default Effect, Scarcity Bias
Social Proof	Activity Message	Informing the user about the activity on the website (e.g., purchases, views, visits)	313	264	○	◐	◐	○	○	Bandwagon Effect
	Testimonials	Testimonials on a product page whose origin is unclear	12	12	○	○	◐	○	○	Bandwagon Effect
Scarcity	Low-stock Message	Indicating to users that limited quantities of a product are available, increasing its desirability	632	581	○	◐	◐	◐	○	Scarcity Bias
	High-demand Message	Indicating to users that a product is in high-demand and likely to sell out soon, increasing its desirability	47	43	○	◐	○	○	○	Scarcity Bias
Obstruction	Hard to Cancel	Making it easy for the user to sign up for a service but hard to cancel it	31	31	○	○	○	◐	●	None
Forced Action	Forced Enrollment	Coercing users to create accounts or share their information to complete their tasks	6	6	●	○	○	○	●	None

From: A. Mathur, G. Acar, M.J. Friedman, E. Lucherini, J. Mayer, M. Chetty and A. Narayanan, Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, in CSCW, article 81, 2019.

2.4. *What can be done against dark patterns?*

Logically, the first step is to become aware of their existence, which, as mentioned previously, is often hard to detect. Drawing on the abovementioned research of Nobel Prize winner Daniel Kahneman, we, as people and consumers, must direct our personal effort towards enhancing system (2) of thinking, thereby avoiding system (1) characterized by quick and intuitive decision-making. This implies a de-biasing effort.

Undoubtedly, the personal effort required is going to be titanic, because we, as consumers, will face an army of designers equipped with knowledge of our biases and manipulability. This is clearly confirmed by some publications that list hundreds of intelligent design strategies based on people's way of thinking.[28]

[28] S. M. Weinschenk, *100 Things Every Designer Needs*

It is therefore necessary to reflect on whether people can be left alone against such evil architects of their choices; whether or not they can be involved in a David-Goliath struggle in which they represent the former, the one that rarely wins.

2.5. *What kind of public scrutiny can be exercised over dark patterns? What is the existing regulation of dark patterns in the European Union and the United States?*

In view of the above and given that dark pattern development actually involves market faults and corporate abusive practices, public interventions against them seem necessary.

Obviously, there can be different types of intervention, ranging from sermons to carrots and sticks.[29] Thus, public interventions can involve consumer information campaigns and promotion of companies' self-regulation (something that the EU has been trying with relatively limited success —in view of how widespread these practices are— since 2018 with the Code of Disinformation Practices[30]), as well as the legal regulation of digital decision architecture (by prohibiting and by establishing specific requirements for consumer protection, including the definition, where appropriate, of infringements and penalties —traditional "command and control" activity).

Both the European Union and the United States have regulations on dark patterns, but their approach is different.

In the US, some laws that specifically define and prohibit dark patterns are coming into force, as in the case of the State of California, as we have seen before.

Conversely, in the European Union there is neither a definition of the phenomenon nor an ad-hoc regulation yet. Several voices seem to agree that this would not be necessary, since existing European norms on data protection and consumer protection already regulate it in general terms.[31]

2.6. *What issues regarding dark patterns remain open?*

Shedding more light on dark patterns is necessary, especially in the case of the European Union, but it also essential to reflect on some questions that remain still unanswered, such as:

Do dark patterns subsist because of the absence of specific regulation or due to the lack of effective enforcement of existing general regulation in areas such as data protection or consumer protection?

Is self-regulation —like the EU Code of Disinformation Practices— a truly effective instrument in this area? Which model can be more effective, the American model of prohibition and explicit regulation, or the European one? Are there enough mechanisms in place in the EU to develop effective public policies against dark patterns? If not, what should be done in the future?

Finally, although the analysis of artificial intelligence has been excluded from this first reflection, it is impossible not to wonder what the use of machine-learning algorithms in combination with nudges will bring in the near future. "Darker" patterns? Does the recent proposal for EU Regulation in the field of Artificial Intelligence address this question? Should it? Or is it a question for the future Digital Services Act?

In that regard, European Parliament included amendments in the original text of this bill at the beginning of 2022 banning dark patterns.[32]

---

to Know about People, Indianapolis, IN, New Riders Publishing, 2011.

[29] R. Rist, Carrots, Sticks and Sermons. Policy Instruments and Their Evaluation, London, Routledge, 2003.

[30] See the text of the Code at Code of Practice on Disinformation | Shaping Europe's digital future, in www.archive-it.org.

[31] S. Rieger and C. Sinders, *Dark Patterns: Regulating Digital Design*, Stiftung Neue Verantwortung, 2020; S. Berbece, *Let There Be Light! Dark Patterns Under the Lens of the EU Legal Framework*, KU Leuven Student Master´s work, 2019, available at SSRN: https://ssrn.com/abstract=3472316.

[32] Specifically, the amendments are the following:
Amendment 105 introduces a proposal for a new regulation of article 2 – paragraph 1 – point q a: "(qa) 'dark pattern' means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice".
Amendment 158 introduces a proposal for a new regulation of article 12 – paragraph 2 c: "2c. Providers of intermediary services shall refrain from any dark patterns or other techniques to encourage the acceptance of terms and conditions, including giving consent to sharing personal and non-personal data".
Short justification included in the *Opinion of The Committee on Civil Liberties, Justice and Home Affairs* (28 July 2021): "Behavioural and personalised targeting for non-commercial and political advertising should be phased out to protect users and ensure the existence of traditional media, and be replaced by contextual advertising. The same should apply to targeting people based on sensitive data, or to targeting minors. Behavioural and personalised targeting for commercial advertising should only be possible where users have freely opted in, without exposure to 'dark' patterns or the risk of be-

After considering the problem of dark patterns and the possible legal solutions, the second part of this reflection will focus on the role of Artificial Intelligence and public intervention specifically.

3. *Decision architecture and digital nudges. Are they against humanity?*

The previous section introduced the idea that digital decision architectures and the use of digital nudges can represent serious risks of manipulation, as was declared to be the case by the Council of Europe in 2019, as we have seen. However, the focus of that reflection was on their use by the private sector, on the so-called dark patterns, thus no specific reference was made to artificial intelligence.

In this part, the analysis will be complemented by adding the public sector and AI to the discussion on possibilities and risks related to digital nudging.

3.1. *The great digital manipulation of our cognitive biases in the attention economy*

As mentioned in the previous section, the use of nudges, whether digital or not, does not necessarily imply manipulation or opacity. Digital nudges can be perfectly ethical and lawful, transparent, and encourage the consumption of "desirable" products or the pursuit of the general interest. Actually, in the case of governments and public administrations, digital nudges if transparent and design respecting the law can be an element of promoting the right to good administration, by serving people with a citizen-centric approach.[33]

Unfortunately, in the case of private sector, according to some authoritative voices, like Williams[34] currently digital nudges imply a

ing excluded from services, and without being fatigued by consent banners if they have already made a clear choice in their browser/device settings".

Amendment 11, proposal for a new regulation of Recital 15 b: "(15b) Targeting individuals based on personal data, including behavioural data, should not be permitted for non-commercial and political purposes. Misleading or obscure advertising for non-commercial and political purposes is a special class of online threat because it influences the core mechanisms that enable the functioning of our democratic society. Targeting minors on the basis of their personal data or targeting individuals on the basis of special categories of data which allow for targeting vulnerable groups should not be permitted. Targeting recipients for commercial purposes should require the recipients' consent. To ensure that recipients have a real choice, refusing consent should be no more complicated than giving consent, "dark patterns" should not be used to undermine the recipient's choice and refusing consent should not result in access to the functionalities of the platform being disabled. In order to avoid fatiguing recipients who refuse to consent, terminal equipment settings that signal an objection to processing of personal data should be respected. Displaying contextual advertisements does not require processing personal data and is thus less intrusive".

According to amendment 40, introducing a proposal for a new Recital 39: "(39a) Recipients of a service should be able to make a free, autonomous and informed decisions or choices when using a service and providers of intermediary services shall not use any means, including via its interface, to distort or impair that decision-making. In particular, recipients of the service should be empowered to make such decision sinter alia regarding the acceptance of and changes to terms and conditions, advertising practices, privacy and other settings, recommender systems when interacting with intermediary services. However, certain practices typically exploit cognitive biases and prompt recipients of the service to purchase goods and services that they do not want or to reveal personal information they would prefer not to disclose. Therefore, providers of intermediary services should be prohibited from deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof ('dark patterns'). This should include, but should not be limited to, exploitative design choices to direct the recipient to actions that benefit the provider of intermediary services, but which may not be in the recipients' interests, presenting choices in a non-neutral manner, such as giving more visual prominence to a consent option, repetitively requesting or urging the recipient to make a decision such as making the procedure of cancelling a service significantly more cumbersome than signing up to it. However, rules preventing dark patterns should not be understood as preventing providers to interact directly with users and to offer new or additional services to them. In particular it should be possible to approach a user again in a reasonable time, even if the user had denied consent for specific data processing purposes, in accordance with Regulation (EU) 2016/679. The Commission should be empowered to adopt a delegated act to define practices that could be considered as dark patterns".

The Explanatory statement underlines that: "In addition, the Rapporteur believes that the algorithms used in recommender system should be designed in a way that prevents dark patterns and rabbit holes from happening. Moreover, the Rapporteur suggest a "must-carry" obligation to ensure that information of public interest is high-ranked in the platform's algorithms".

[33] J. Ponce (ed.), *Nudges, Good Governance and Good Administration. Behavioral Insights, Nudging and Public and Private Sectors*, Athens, European Public Law Organization (EPLO), 2022 (upcoming book, soon to be published).

[34] In this section, I will consider the remarkable reflections offered by James Williams' book, *Stand out of our Light. Freedom and Resistance in the Attention Economy*, Cambridge, Cambridge University Press, 2018. This interesting publication of the co-founder of "Time Well Spent" —a movement that led to the creation of the Center for Humane Technology— won the Nine Dots Award. James Williams worked as a strategist at Google

large-scale manipulation project that has been undergoing development for a long time and which has barely been recognized until now. This project recalls religious/mythical/totalitarian systems, is in the hands of very few people in the world and is aimed at the consumer: an objective pursued by spending huge amounts of money on advertising (in 2017 advertising expenditure was 223 billion and it is growing by 10% annually). Consumers, as said, are the target of cognitive biases' manipulations and this has also been reported by Williams, who explicitly cites Kahneman and Tzaversky in support.

This large-scale system of manipulation operates in the attention economy, an environment in which digital products and services compete relentlessly to capture and exploit consumers' attention.[35] Obviously, the same risk in the case of the public sector can be also identified for other purposes.[36]

3.2. *Digital manipulation against the right to freedom of thought, the dignity of the person, free development of the personality and the Social and Democratic Rule of Law*

It is important to underline that attention is linked to freedom and human will, and the system of large-scale manipulation by digital design that has been described harms both.

First of all, this is because that there cannot be freedom of thought without freedom of attention. In the classic "On Liberty", John Stuart Mill's book published in 1859, already explained a very similar concept about freedom of thought (p. 15 ff.):

"It comprises, first, the inward domain of consciousness; demanding liberty of conscience in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological. The liberty of expressing and publishing opinions may seem to fall under a different principle, since it belongs to that part of the conduct of an individual which concerns other people; but, being almost of as much importance as the liberty of thought itself, and resting in great part on the same reasons, is practically inseparable from it. Secondly, the principle requires liberty of tastes and pursuits; of framing the plan of our life to suit our own character; of doing as we like, subject to such consequences as may follow: without impediment from our fellow creatures, so long as what we do does not harm them, even though they should think our conduct foolish, perverse, or wrong.

[…]

Not that it is solely, or chiefly, to form great thinkers, that freedom of thinking is required. On the contrary, it is as much and even more indispensable to enable average human beings to attain the mental stature which they are capable of".

When digital interactions manipulate the freedom of attention, they also affect the freedom of thought: a right to freedom protected by the Universal Declaration of Human Rights and the European Convention of Human Rights (art. 9).

Taking the Spanish case as an example, although the Spanish Constitution does not explicitly mention this right, it can be assumed that its art. 20, which safeguards the freedom of expression, also protects the freedom of thought. In addition, as recalled by the Spanish Constitutional Court in sentence number 76/2019, the ideological freedom guaranteed by art. 16.1 of the Spanish Constitution has two dimensions: one is internal and involves the right to adopt a certain intellectual position before life and other life-related issues, and to represent or judge reality according to personal convictions. The other, the external one, is the dimension of *agere licere*: the right to act according to one's own ideas without incurring any penalty or demerit and without suffering compulsion or interference on the part of public authorities.

Therefore, it can be said that a —public or private— digital design that takes advantage of biases to manipulate and capture people's attention can undermine their constitutional

for 10 years and, as a result of this experience, he decided to leave the company to pursue a PhD at Oxford and conduct research on the philosophy and ethics of technology.

[35] "…when we use the term "attention" in day-to-day parlance, we typically mean what cognitive scientists call the "spotlight" of attention, or the direction of our moment-to-moment awareness within the immediate task domain", J. Williams, *Stand out of our Light*, 44-45.

[36] *The Guardian*, article published in 8 September 2021, underlines in relation to UK government that some studies show a growing government use of sensitive data to nudge behaviour. See *TechScape: Should government use the web to nudge our behaviour? | Technology | The Guardian,* in www.theguardian.com.

right to freedom of thought, which is intimately linked to the value of dignity and to the freedom of development of one's personality (following with the Spanish example, art. 10.1 of the Spanish Constitution).

The second reason is that this manipulation of attention implies hindering human will. There can be no human will without attention, because will, which is the faculty of deciding and ordering one's own conduct, can only exist if there is attention and absence of manipulation. From a legal standpoint, digital manipulation can thus be considered a threat to the freedom of individuals to establish rules of conduct for themselves and others within the limits of the law, hence, an impediment to the autonomy of the will safeguarded by many legal systems (using again the example of Spain, by art. 1255 of the Civil Code).

Thirdly, it should be noted that if freedom of thought and individual will be played upon through the digital manipulation of millions of people, then the general will is also affected, thus damaging democracy and the rule of law. Accordingly, in the decision cited above — and in many other similar cases— the Spanish Constitutional Court has stressed that, without freedom of thought, neither would there be a place for the fundamental principles of a legal system based on democratic values and the rule of law.

3.3. *An anti-Enlightenment project: modes of digital manipulation*

The attention economy and digital manipulation harm both people and social, legal and political systems. Their negative impact is therefore not trivial. The stakes are high.

In his abovementioned book, Williams[37] proposes a useful threefold distinction about this harmful effect to understand it better: the impact on "the doing" (that he calls spotlight), the impact on "the being" (on the values that guide us, which he calls starlight) and the impact on "the knowing" (which he calls daylight):

Digital manipulation and distractions of attention regarding "the doing". This is the typical loss of concentration due to digital designs aimed at distracting the individual (with the awareness that, after each distraction, attention is generally recovered in approximately 23 minutes). The author points out that the impact on "the doing" is not only individual: it can also have social significance, as it may affect political life. In fact, digital designs can distract from the relevant information that allows one to be politically informed. Among the examples provided by Williams there are practices implemented by China and the former US President Donald Trump. This type of manipulation, however, is not the only form in the digital environment and, although serious, it is not the most corrosive for democratic coexistence.

Digital manipulation and distractions of attention regarding "the being". This second type of digital distraction is aimed at making people lose their values through the promotion of pettiness (that is, the assignment of intrinsic value to goals and objectives with no intrinsic value, that are often marked by a poverty of spirit and short-sightedness, and which reveal lack of prudence), narcissism and social fragmentation, with the consequent erosion of values such as social cohesion.

Digital manipulation and distractions of rationality regarding "the knowing". According to the author this is the "epistemic distraction", which affects reflection, memory, prediction, calm, logic and goal-setting. The digital environment does this through fake news, impairment of intelligence and emotional capacities, by generating stress and other pathologies, by affecting reflection through notifications and applications, by promoting continuous moral indignation and by leading to dehumanization and populism. Accordingly, several studies have led Nicholas Carr to declare to the BBC that we are becoming less intelligent, more closed-minded and intellectually limited by technology.[38] A technique at the service of this impairment of the "daylight" is precisely the use of dark patterns already addressed in the previous section.

It should also be recalled that in a well-known article written in 1784, Kant pointed out that enlightenment is characterized by the decision and the courage to use one's own understanding without the guidance of others; the famous *sapere aude*, which can bring people out of a self-guilty dependence caused by laziness and cowardice.[39] Centuries later,

[37] J. Williams, *Stand out of our Light*, 2018.

[38] See Nicholas Carr: "Nos estamos volviendo menos inteligentes, más cerrados de mente e intelectualmente limitados por la tecnología", in *BBC News Mundo*.

[39] *Beantwortung der Frage: Was ist Aufklärung?*, often

these concepts have become topical again because of digital manipulation: a market-driven project for bringing us back to dependence by means of distractions that sap our attention, and hidden nudges that push us where we don't want to go.

Therefore, digital manipulation can be seen as an "anti-Enlightenment" project.

3.4. *Compulsion Incentivizing Technologies. The impact of Artificial Intelligence (AI)*

In other words, and in relation to what has been said in the previous section, digital manipulation acts by taking advantage of biases, by playing upon them, by exploiting and enhancing system 1 of thinking and by deactivating system 2.

This scenario is likely to get worse in the future, for at least two reasons. The first is the potential increase in available leisure and the consequent rise in consumption of technologies that incentivize compulsion.

Secondly, because of the impact of AI. In this regard, Yeung has introduced the concept of "hypernudge": nudging empowered by Big Data and algorithms that has the ability to move from the one-size-fits-all design to "tailored" —precision— nudges, which target specific individuals according to their specific characteristics through machine learning.[40]

Yeung warned that Big Data-driven nudging is agile, discreet and very powerful. It provides data holders with the ability to generate a highly personalized choice architecture by guiding people's decisions, no matter whether they are consumers or users of a public service. In fact, the author conceives hypernudges as instruments of control based on design and, to give a straightforward example about them, she pointed to the order of the results pages provided by search engines —e.g. Google, Bing etc. These instruments do not force us to look only at the first websites of the list —which happen to be also the most favourable for search engine marketing—, nor to forgo the other hundreds of thousands of websites, but that is exactly what we do, and the search engine knows that, because of our cognitive and temporal limitations.

The hypernudge is based on the highlighting of algorithmically determined correlations between elements of data that human cognition cannot observe, not even with the help of standard computing technology. This confers an undisputed prominence to the highlighted data patterns, as they allow the dynamic configuration of the informational choice of the user and her/his decisions to be swayed by taking advantage of priming: the psychological effect whereby the exposure to one stimulus —e.g. images, sounds, words etc.— influences the response to a subsequent stimulus, hence also future behaviours and actions.

Big Data-driven nudging can be very useful in medicine[41] and public services management,[42] but also in fields like tax compliance and tax administration, as proved by the example of the Strategic Plan 2020-2023 designed by the Spanish Tax Agency.[43]

Nevertheless, it should not be overlooked that Big Data-driven nudging can also put people's rights at risk.

This is particularly evident in terms of personal data protection, as remarked by the District Court of The Hague at the beginning of 2020 with an express mention of art. 8 of the European Convention on Human Rights (ECHR).[44] In the case in question, SyRI, the Dutch algorithmic System for Risk Indication, and the public authorities that implemented and managed it, stood —and were— accused of having collected, for several years, a disproportionate amount of taxpayers' personal data —on income, pensions, insurance, type of house, taxes, fines, integration, education, debts and

referred to simply as "What Is Enlightenment?", is a 1784 essay, published in December 1784 in the *Berlinische Monatsschrift* (*Berlin Monthly*).

[40] K. Yeung 'Hypernudge': Big Data as a mode of regulation by design, Information, in Communication & Society, vol. 20, issue 1, 2017, 118.

[41] D. Misawa, J. Fukuyoshi and S. Sengoku, Cancer Prevention Using Machine Learning, Nudge Theory and Social Impact Bond, in International Journal of Environmental Research and Public Health, vol. 17, No. 3, 2020, 790.

[42] J. Ponce, El derecho a una buena administración y la personalización de los servicios públicos. Sesgos, "nudging" e inteligencia artificial in B. Puentes Cociña and A. Quintiá Pastrana (eds.), El derecho ante la transformación digital: oportunidades, riesgos y garantías, Barcellona, Atelier, 2019, 51.

[43] See the *Strategic Plan 2020-2023* of the Spanish Tax Agency at: *adenda_plan_objetivos.pdf*, in www.agenciatributaria.es.

[44] On 5 February 2020, the District Court of The Hague (*Rechtbank Den Haag*) held that the System Risk Indication (SyRI) algorithm system, a legal instrument that the Dutch government uses to detect fraud in areas such as benefits, allowances, and taxes, violates article 8 of the European Convention on Human Rights (ECHR) (right to respect for private and family life).

unemployment benefits— to calculate who was more likely to defraud the welfare system

Personal data, however, are not the only things at stake. Yeung highlighted that manipulation and deception are another two critical issues and that users' acceptance of information and requests for consent for the use of digital environments are not apt to solve them. This ties in with the potential violation of the right to freedom of thought and of the democratic principles already mentioned.

It is therefore clear that adequate mechanisms to prevent these serious digital risks must urgently be designed.

3.5. *What should —and should not— be done?*

In the light of the situation described above and of the likelihood of dangerous future developments, it is useful to consider the *Onlife Manifesto* funded by the European Commission,[45] which emphasizes that:

"In the digital economy, attention is approached as a commodity to be exchanged on the market place, or to be channelled in work processes. But this instrumental approach to attention neglects the social and political dimensions of it, i.e., the fact that the ability and the right to focus our own attention is a critical and necessary condition for autonomy, responsibility, reflexivity, plurality, engaged presence, and a sense of meaning. To the same extent that organs should not be exchanged on the market place, our attentional capabilities deserve protective treatment. Respect for attention should be linked to fundamental rights such as privacy and bodily integrity, as attentional capability is an inherent element of the relational self for the role it plays in the development of language, empathy, and collaboration. We believe that, in addition to offering informed choices, the default settings and other designed aspects of our technologies should respect and protect attentional capabilities".

As already pointed out, defending attention from manipulation and deception means defending freedom of thought and human will, both at the individual and at the collective level. This is a political task that requires a prior reform of the current totalitarian system of information technologies, because digital design is the politics behind the politics.

Before proposing concrete measures, there are some actions and attitudes that should be avoided in order to face the described dangers. "Doing nothing" is the first inadvisable posture, because the existing evidence suggests the need to take an active and precautionary approach (based on the precautionary principle) towards technologies, especially in the social sphere. Neither can the problem be solved by advising users to disconnect or adapt to the current situation. Moreover, we consider it unwise and inconvenient to rely only on technological companies' self-regulation and ethics, as these can be just a facade and an attempt to push aside the law.[46]

Then what should be done? The solution lies in the introduction of incentives for technology design that benefit consumers and users and contribute to making technologies more human.

The main interventions that could help move the attention economy in the right direction are: (1) rethinking the nature and purpose of advertising, (2) conceptual and linguistic reengineering, (3) changing the upstream determinants of design, and (4) advancing mechanisms for accountability, transparency and measurement.

Advertising: in this field, Williams, in his book, suggests make ad blocking software mandatory and activated by default, with users being able to unblock it if they wish. Thus, although he does not use the term "nudge", this is exactly what he means by proposing a default option or, more specifically, an opt-in: not receiving advertising unless I choose to receive it. This is an important proposal that leads us to reflect as well on the legal battle that has been going on for years against Internet ad-blocking applications.[47]

Language: Williams identifies various terms related to the language of digital persuasion, which he groups into triads, from lesser to greater impact on people's attention and will: invite-tempt-seduce / suggest-persuade-demand / direct-guide-drive. It is necessary to make progress in specifying what

[45] See L. Floridi, The Onlife Manifesto. Being Human in a Hyperconnected Era, Berlin, Springer, 2015,13, § 4.6, open access at: The Onlife Manifesto | SpringerLink.

[46] See the interview with Prof. Karen Young at *AI and the law*, in www.birmingham.ac.uk.

[47] A.M. Russell, *The Legal Fate of Internet Ad-Blocking*, in Boston University Journal of Science & Technology Law, 24, 2018, 299.

these contexts of persuasion are, because, as Wittgenstein said, "the limits of my language mean the limits of my world (*Tractatus Logico-Philosophicus*, proposition 5.6)." In order to achieve a more human design of technologies it is therefore overwhelmingly important to name, classify and reflect on digital nudges.[48]

Modification of technological design: policymakers should have a fundamental role to play in responding to the crisis of the digital attention economy. We can take inspiration from pre-digital regulations on junk mail or telemarketing calls, which, after all, tried to avoid unwanted intrusions into private life. Transparency about the objectives of digital design is paramount.[49]

Examples of how policymakers and judges can protect citizens from manipulation and digital deception are already observable. Some of them can be found in the decision of 1st October 2019 from the Court of Justice of the European Union (CJEU), Grand Chamber, in which it was established that the existence of genuine consent implies avoiding ticked boxes by default, in accordance with EU Law (Privacy Directive 2002/58/EC, art. 6 GDPR and Directive 95/46/EC).[50]

Another interesting line of intervention could be creating digital media platforms that could play a similar role to the one that public broadcasting has played in television and radio. In accordance with this approach, which regards the provision of digital public services to counteract the aforementioned manipulations and increase the "lights" (that nonetheless should be controlled for their potential to create similar risks), it is worth drawing attention to the Italian experience ITsART.[51] This is a new platform promoted by the Italian Ministry of Culture and *Cassa Depositi e Prestiti* (Italy's deposits and loans fund) for world-wide distribution of artistic and cultural content in digital form. The business partner of the project is CHILI Spa, a company selected for its industrial and technological know-how. ITsART is managed through a company with 51% public shareholding; a public-private partnership in which CHILI Spa only owns 49% of shares.

The latter proposal challenges the widespread idea that the state should always withdraw from the provision of public services and become a mere guarantor or regulator, given its shortcomings and inadequacies vis-à-vis the private sector. This is neither true nor necessary in all cases, unless it is advocated with a specific ideological goal, as the Nobel Prize winner Herbert Simon pointed out some time ago.[52] Avoiding such an ideological bias is crucial, as well as analysing on a case-by-case basis if the intervention of Administrations is to become necessary and apt to serve the general interest, both in the digital world and outside it. The idea of a formal democracy as a guarantor of formal rights and freedoms must give way to a material democracy that enables everyone to enjoy such rights and freedoms on an egalitarian basis; something that would be impossible without reinforcing the principle of equality. Freedom without equality is an empty concept. Hence the need for governments to direct economic life and to strive for the achievement of the maximum general welfare.

Accountability and measurement: although blaming designers for lowering our "lights" is unwise —as it is the result of a systemic functioning that incentivizes manipulation—, the introduction of a professional oath for digital designers, similar to the Hippocratic Oath, may be a good option, according to Williams. However, he also admits that its implementation would not be free of complications, especially due to the plurality of professions involved in digital design, including people without specific training, and

[48] J. Williams, *Stand out of our Light*, 114: "Clarifying the language of persuasion will have the added benefit of ensuring that we don't implicitly anchor the design ethics of attention and persuasion in questions of addiction", which is a core problem, but also "a convenient distraction from deeper questions about a design's fundamental purpose".

[49] In his book, William goes so far as to propose the introduction of a fee for exceeding certain levels of "attention offsets". This idea, which implies punishing companies for provoking intentional harm, was not further detailed and developed by the author; nevertheless, it clearly reflects the important role that the law should play.

[50] It is precisely due to these regulations that, in 2014, Spain added art. 60 *bis* to the Royal Legislative Decree 1/2007, of 16th November, which approved the revised text of the General Law for the Defence of Consumers and Users and other complementary laws. In particular, art. 60 *bis* establishes that consumers and users are entitled to the reimbursement of additional payments charged by the trader without their express consent through default options.

[51] See www.ITsART.tv.

[52] As the Nobel Prize winner Herbert Simon pointed out some time ago, H.A. Simon, *Why Public Administration?,* in *Journal of Public Administration Research and Theory*, vol. 8, issue 1, January 1998, 1.

the lack of professional associations.[53]

3.6. *Inadequacies of ethics and self-regulation (even regulated): lobbies and regulation*

It is now clear that the combination of digital design, *nudges* (including dark patterns), exploitation of cognitive biases, Big Data and AI can create an explosive cocktail for citizens' freedom and free will and for the functioning of social and democratic states governed by the rule of law. Nevertheless, we should not "throw the baby out with the bathwater" and deny or waste the potential of all these techniques and technologies to serve the general interest. It seems clear that threats to democracy and people's rights described above cannot be tackled merely through private companies' self-regulation and enthusiastic calls for ethics; just as serious illnesses cannot be cured with love and prayer alone.

The role of law and, within it, of "positive nudges" in defence of citizens is an issue more pressing than ever. In Europe we have already had bitter experiences with self-regulation — including regulated self-regulation—, for example, in the banking sector. This was made clear by the Great Recession and the European Commission recognized it, by pointing out that financial actors have wrongly determined their actions and business policies with dire consequences.[54]

Hopefully, the same mistakes will not be repeated in the digital sphere, and the frustrations generated by the ineffectiveness of self-regulation will be learnt from, as in the case of the EU Disinformation Code mentioned in the previous section. This example of self-regulation has been assessed by the European Commission, which considers that the assessment "has revealed significant shortcomings. These include inconsistent and incomplete application of the Code across platforms and Member States, limitations intrinsic to the self-regulatory nature of the Code, as well as gaps in the coverage of the Code's commitments. The assessment also highlighted the lack of an appropriate monitoring mechanism (…), lack of commitments on access to platforms' data for research on disinformation and limited participation from stakeholders, in particular from the advertising sector". Therefore, the European Commission concludes that it is necessary "to transform the Code into a stronger instrument for addressing disinformation and creating a safer and more transparent online environment".

In the same line, the OECD has pointed out that "Industry self-regulation can be an advantageous complement to government policies, but it also poses a number of challenges" and that "the use of ISR to help address consumer issues needs to be considered systematically when policy makers and enforcement authorities are developing options for taking action. As discussed in the Consumer Policy Toolkit, ISR could be part of a multi-faceted response to a problem, supporting other measures that governments might take. With respect to the development, monitoring and evaluation of such mechanisms, it appears that stakeholder involvement has been limited, and that it may be beneficial to explore whether there are ways that involvement could be strengthened, in ways that would benefit all stakeholders".[55]

Although powerful market forces opposed to regulation in the general interest will probably continue to act as lobbies against a stronger regulation when and if necessary, it is a matter of being timely and avoiding large-scale opaque and negative psychological mutation of consumers, citizens and democratic political systems.

The future European regulation on AI offers an ideal opportunity to discuss these issues, and hence to go beyond the necessary but insufficient concern for personal data protection.[56] Title II of the proposal of regulation made public in April 2021 sets out a list of prohibited AIs. This draft regulation follows a risk-based approach by differentiating between AI uses that constitute (i) unacceptable risk, (ii) high risk, and (iii) low or minimal risk. The list of prohibited practices included in Title II comprises all

[53] To overcome them, the author suggests how to elaborate the oath and what content it should have, making a concrete proposal: J. Williams, *Stand out of our Light*, 120.

[54] European Commission, Green Paper - Corporate governance in financial institutions and remuneration policies {COM(2010) 286 final} {SEC(2010) 669}.

[55] OECD, Industry Self-Regulation: Role and Use in Supporting Consumer Interests, 2015, available at: Industry Self-Regulation: Role and Use in Supporting Consumer Interests, in www.oecd.org.

[56] See the regulation at Proposal for a Regulation laying down harmonised rules on artificial intelligence | Shaping Europe's digital future, in www.europa.eu.

those AI systems whose use is considered unacceptable because they contravene EU values; among them, "the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm" (art. 5.1.a)

It should be also noted that the proposal points out that other manipulative or exploitative practices facilitated by AI systems could be covered by data protection, consumer protection and digital services legislation ensuring that individuals are properly informed and can freely choose not to be subjected to profiling or other practices that may affect their behaviour.

The reference to physical or psychological harm, however, is not particularly appropriate, given the significance of digital designs in relation to potentially manipulative AI. This should be replaced by a simple mention of the possibility of causing or inducing error or deception, thereby affecting the autonomy of the will. In this regard, it was mentioned in the previous section about the recent amendment of the California Privacy Rights Act (CPRA) of 2020 to ban dark patterns.

Accordingly, it would also be worth reformulating the European draft regulation by including a ban on any AI system that deploys subliminal techniques beyond a person's consciousness in order to distort her/his behaviour to subvert or impair her/his autonomy, decision making or choice. This is the line of the amendments to the draft of the Digital Services Act introduced by the European Parliament in January 2022, banning dark patterns, as we have seen above.

4. *Conclusions*

The use of behavioural insights in the digital domain has become extremely significant during the COVID-19 pandemic. Although digital nudging can be useful for making effective the right to good administration, it can create unacceptable manipulations. In this area, the possible use by the public and private sector of the so-called dark patterns, concerning which the European Parliament has recently proposed to include a ban in the future Digital Services Act, and what is known as hypernudging raises legal doubts regarding a possible violation of freedom of thought, as indicated by the Committee of Ministers of the Council of Europe in a recent statement of 2019. The future Digital Services and Artificial Intelligence regulations could and should introduce provisions avoiding the worst effects of digital manipulation.

The door is open to use the best of artificial intelligence and to avoid the worst, through reasonable EU and national regulations avoiding that we, the citizens, become digital *zombies* in the hands of governments and corporations.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 45-56
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 04

*Better Decision-Making, Algorithmic Discrimination and Gender Biases: A New Challenge for the Administration of the 21st Century**

Eva Mª Menéndez Sebastián
(Full Professor of Administrative Law at Oviedo University)

With the collaboration of **Belén Mª Mattos Castañeda**
(PhD in Law at Durham University)

ABSTRACT We are currently witnessing a social transformation with various converging factors, among which this article will focus on the new public governance and the incorporation of artificial intelligence. This work proposes an analysis of the connection between these two spheres and, in particular, two elements: good administration and the employment of algorithms by the Public Administration. The aim is to highlight the necessity to regulate this instrument and adopt preventive and control mechanisms, in order to avoid algorithmic discrimination, especially from a gender-sensitive perspective.

1. *Problem statement*

The role played by the Administration and its relationship with the citizens are extremely relevant in a State of social democracy, subject to the Rule of Law.[1] This premise has gained special significance and meaning in recent times, with the impetus of what has been called *new public governance*.

To begin with, some fundamental aspects of this phenomenon will be succinctly outlined. *Good government*, *good administration*, and *good regulation* are three concepts inherent to this idea of *new public governance*. This article will not address the differences between these three notions in detail, and previous works may be consulted for further reference.[2] Here it will be sufficient to underline that it is possible to make a distinction between the three concepts aforementioned. The difference is not merely regarding the subject but rather the technical or political nature of the decision. However, these notions share common features, in particular, the importance of certain principles and aims.

In terms of the aims, the idea of *public governance* should be connected or based on two essential elements or objectives: regaining the confidence of citizens in the institutions and putting into practice what the French doctrine denominates as *administrative citizenship*, which will be addressed later in this work. The key idea is that the Public Administration is at the service of citizens and, therefore, citizens can control it. In order to do this, they must be able to learn about it (transparency), get involved in the decision-making process (participation), and evaluate its performance (accountability).

Within this idea of public governance, there are some principles that are particularly worthy of attention, such as transparency,[3] participation,[4] accountability,[5] public ethic

* Article submitted to double-blind peer review.
This research is part of the work of the Rafael del Riego Chair of Good Governance, directed by Eva Mª Menéndez Sebastián, and the project TED2021-129283B-I00, funded by MCIN/AEI/10.13039/501100011033 and the European Union NextGenerationEU/PRTR.

[1] As it has been highlighted in E.Mª. Menéndez Sebastián, *La Administración al servicio de la justicia social*, Madrid, Iustel, 2016.

[2] E.Mª. Menéndez Sebastián, *De la función consultiva clásica a la buena administración. Evolución en el Estado Social y Democrático de Derecho*, Madrid, Marcial Pons, 2021; or E.Mª. Menéndez Sebastián and J. Ballina Díaz, *Sostenibilidad social y ciudadanía administrativa digital*, Madrid, REUS, 2022.

[3] This is perhaps the aspect that has been emphasized the most. It responds to the need to know what the Public Administration does in order to be able to control it, and it must be extended to public services as well.

[4] It should be noticed that there are different types of participation and each one of them contributes to good administration, good governance and good regulation, not only by the civil society – which has knowledge about its needs –, but also by interest groups or experts, whose knowledge contributes to greater success in decision-making. There are also different types of participation according to the moment when it takes place. For instance, deliberative participation

and integrity,[6] open data,[7] effectiveness and efficiency,[8] innovation,[9] and equality and non-discrimination.[10]

Therefore, a strategy of *public governance* that aims at being global, comprehensive, and inclusive must adopt this approach and, especially, a gender-sensitive perspective. This aspect is related to the achievement of the Sustainable Development Goals set by the 2030 Agenda, specifically goals no. 5, 10, 16, and 17. These refer to gender equality, reduction of inequalities, peace, justice and strong institutions, and multi-stakeholder partnership, respectively, all of which inform the core concept of *social sustainability.*[11]

This is the approach that this work will employ without losing sight of the fact that the use of artificial intelligence and, in particular, algorithms in administrative decision-making has been called into question, not only concerning non-participation but also the violation of the principle of equality and non-discrimination.

2. *The citoyenneté administrative: a key French notion*

The term *administrative citizenship*[12] proposed by the French doctrine reflects the transformation of the consideration of an individual who has a relationship with the Public Administration or uses a public service from subject or user[13] to citizen. Likewise, it

(determining what is of general interest for citizens, i.e. issues to be addressed), participation in decision-making (participation in the strictest sense, this is, in the elaboration of norms, the political decision-making, and the Administration as well), and participation in the evaluation of those decisions and their results.

[5] Evaluating decisions is important to determine their effectiveness, thereby changing or maintaining them. Accountability – which may also be considered as participation from a broad perspective – is extremely relevant, and this might be the least studied aspect of the three notions that usually encompass the concept of *public governance*. In this regard, it is noteworthy the recent study conducted by the French Conseil d'État on this subject: *Etude annuelle 2020. Conduire et partager l'évaluation des politiques publiques*, La Documentation Française, Paris, 2020. This issue is also connected with what has been denominated as legal experiments, *clauses de réexamen*, *review clauses, sunset clause o clause crépusculaire* and has been explored in works such as A. Boto Álvarez, *Experimentación regulatoria: la introducción de proyectos pilotos de excepción en el sector eléctrico español*, in M. Anglés Hernández and M. Palomino Guerrero (eds.), *Justicia energética y sector eléctrico iberoaméricano*, México, UNAM, 2021, 161, and in other legal systems more intensively.

[6] Measures in this area are essential to restore public confidence in the institutions. This principle is also related to current issues such as codes of conduct; interest groups, their registration and the legislative footprint file – which is one of the regulatory commitments of the IV Open Government Plan in Spain; revolving doors; conflicts of interest, etc. For further information, see: J. Ballina Díaz, *La formalización de las relaciones entre las instituciones europeas y los grupos de interés: encuentros y desencuentros*, in Mª.P. Andrés Saénz De Santa María (ed.), *Una contribución a la europeización de la ciencia jurídica*: *Estudios sobre la Unión Europea*, Navarra, Thomson Reuters-Civitas, 2019; Id., *La información sobre los grupos de interés comunitarios: un campo prometedor para el big data*, in A. Huergo Lora and G.M. Díaz González (eds.), *La regulación de los algoritmos*, Navarra, Thomson Reuters Aranzadi, 2020; and J. Ponce Solé, *Mejora de la regulación, lobbies y huella normativa. Un análisis empírico de la informalidad*, Valencia, Tirant lo Blanch, 2019.

[7] The Directive (EU) 2019/1024 on open data and the re-use of public sector information of the European Parliament and of the Council of 20 June 2019 are especially relevant to this topic.

[8] *Good administration* measures are fundamental in this sphere; hence it is necessary to delve into digital transformation, administrative simplification, and organisational issues. Since g*ood government* and *good administration* primarily seek better decision-making these are especially linked to effectiveness and efficiency. In this regard, the general importance of impact assessments, and specifically of *good regulation* must not be overlooked.

[9] In order to satisfy social demands, Administrations must undergo a transformation, from the bureaucratic model to an innovative model, which will allow them to be more effective and efficient. This will lead to the adoption of people-based designs, opting for co-creation, introducing instruments such as *sandbox*, *nudging*, or *innovations lab*.

[10] Equality is not only a clear goal of the 2030 Agenda, but it is also essential to the topic addressed in this work as much of citizens' mistrust in the Administration originates from the perception of inequality. In addition, there can be no adequate *public governance* in a State of social democracy if it is not committed to eradicating inequality. This also entails refraining from taking measures that might increase such inequalities, especially regarding the digital divide, which must be addressed. *Public governance* must be inclusive hence, it is necessary to have a global vision from a gender-sensitive perspective and, more generally, with an approach of non-discrimination.

[11] As has been indicated by the European Economic and Social Committee in its exploratory opinion on "A socially sustainable concept for raising living standards, boosting growth and employment, as well as citizens' security in the digital era" (2018/C 237/01), this issue relates to the capacity to ensure conditions for human well-being (security, health, training, democracy, participation, and justice) equitably distributed between different classes and genders. Therefore, *social sustainability* must be introduced and implemented in the same way as environmental and economic sustainability to reduce inequalities.

[12] On this point see E.Mª. Menéndez Sebastián and J. Ballina Díaz, *Sostenibilidad social y ciudadanía administrativa digital*.

[13] As it has already been pointed out by V. Donier, *Les*

is essential to consider the changes in the classic conception of citizenship itself more attached to the idea of nationality.

The new position acquired by the individual in relation to the Public Administration from a perspective of citizenship justifies an introduction to the principles, which are pivotal to *new governance*. There is a profound transformation of the relationship between the Administration and citizens, formerly considered subjects, in line with what has been considered the transition from *democratic administration* to *administrative democracy*. The increasing use of the notion of *democracy* in Public Administration clearly reflects this change. It entails granting new rights to all citizens and getting them involved in administrative processes within the framework of deliberative and participatory mechanisms.[14]

The issue of *administrative democracy*[15] reflects, in fact, a profound change in the way the relationship between the Public Administration and democracy was traditionally conceived. The former is no longer expected to be democratic but rather to become the spearhead and drive in the reformulation and strengthening of the logic of democracy. However, it is necessary to emphasize that this is complementary to representative democracy and not a substitute[16] and that participation in power does not end with the right to vote and that it extends in a sustained manner.[17] All of this is related to *good administration*,[18] in the sense of efficiency and better decision-making.

This transformation can be noticed in several legal instruments, which have replaced the terms *subject*, *petitioner* or *user* by *citizen*. This in clear in France with *Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations*[19] and, more recently in Spain with *Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas,*[20] or *Ley de Contratos del Sector Público (LCSP)* from 2017.[21]

Therefore, by recognising that the individual formerly conceived as a subject is a citizen, contemporary texts consider that the administrative relationship has a civic dimension. The Administration must provide citizens with the means to exercise their citizenship, and the administrative relationship is one of the means of access to it. This leads to a transformation in the nature of the administrative relationship, with citizens entitled to participate in administrative action and to have access to the Administration, which is held accountable to them.

In these terms, *administrative citizenship* encompasses two fundamental aspects. In the first place, due to the change in the terminology, all of the citizens' rights can be considered now citizenship rights. Secondly, the civic dimension of the administrative relationship is reinforced as a pillar of political citizenship. The emergent *administrative citizenship* entails that electors are at the same time citizens *of* the Administration and citizens *in* the

droits de l'usager et ceux du citoyen, in *Revue française de droit administratif*, vol. 1, 2008, 13, the first step in this evolution was about the idea of the user, demonstrating thus the subject's emancipation, ceasing to be in a subordinate position with the Administration and becoming its beneficiary instead.

[14] According to J. Chevallier, *De l'Administration démocratique à la démocratie administrative*, in *Revue française d'administration publique*, vols. 137-138, 2011, 217.

[15] According to C. Testard, *Pouvoir de décision unilatérale de l'administration et démocratie administrative*, Paris, LGDJ, 2018, this is understood as the set of rules that promote the participation of citizens in the elaboration of administrative decisions.

[16] This is the argument followed by the Conseil d'État, *La citoyenneté. Être (un) citoyen aujourd'hui*, Paris, La Documentation Française, 2018, 14; J. Chevallier, *De l'Administration démocratique à la démocratie administrative*, 227; G. Dumont, *La citoyenneté administrative*, PHD thesis, Université Panthéon-Assas Paris 2, Paris, 2002, 367; and E. Debaets, *Protection des droits fondamentaux et participation de l'individu aux décisions publiques*, in *Jurisdoctoria*, vol. 4, 2010, 175.

[17] A.G. Orofino, *La trasparenza oltre la crisi. Accesso, informatizzazione e controllo cívico*, Bari, Cacucci, 2020, 53.

[18] As has been claimed by the Conseil d'État, *Consulter autrement, participer effectivement*, Paris, La Documentation Française, 2011, 92.

[19] The *Code des relations entre le public et l'administration (CRPA)*, enacted by *Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, JO, n° 0248, 25 octobre 2015, texte n° 2*, 19872, replaces the term "citizen" by that of "public", as has been indicated by F. Pinel, *La participation du citoyen à la décision administrative*, PHD thesis, Université Rennes 1, Rennes, 2018, 19.

[20] This law uses the term "ciudadano" (masculine form of citizen) twenty-one times and only once "ciudadana" (feminine form of citizen), but without explaining the effects terminology shift or making it explicit.

[21] For instance, article 312 refers to services contract with direct benefits to citizenship.

Administration.[22] Finally, the aim is to make citizenship effective through the relationship of citizens with the Administration, this is, with the extended and active participation of citizens in the administrative power.

3. *An approach to good administration*

The aim of this work is not to discuss what is understood by the *notion of good administration*[23] or what it entails in detail. As a paradox, even though this term has been in use for years, not only in jurisprudence but also explicitly in several legal texts,[24] such sources fail to provide a concept or definition of *good administration*. Moreover, this phenomenon occurs in various legal systems.[25]

The absence of a relatively concrete and widely accepted concept caused that the relevance and role of *good administration* have not been recognised, and its practical application has been considerably relegated, despite being a central aspect of Administrative Law. There have been some references to this crucial element of our discipline in jurisprudence recently, but yet excessively timid.

This work argues for granting value to this concept and asserting its importance in the contemporary practice of Administrative Law, stressing the need to provide it with substantial legal effects to connect it with the previously exposed idea of *administrative citizenship*. The role of the European Union in this regard has been remarkable, both through the jurisprudence from the Court of Justice of the European Union (CJEU)[26] and in the indisputable work of the European Ombusman.[27]

There are various perspectives on this point, some of which are fundamental: from the role of *good administration* in the construction of the European administrative area[28] to a more restrictive view[29] that distinguishes it from other terms such as *good government* or *good governance*. Even though Government and Administration have always been closely linked, their functions, approaches, principles, and instruments cannot and should not be identical.

Following this approach, it is possible to offer a concrete notion of *good administration* based on the meaning of the words that compose it and its aim, which is to objectively and effectively serve the general interest.[30] Therefore, there will be *good administration* when it adequately serves the public interest. The adequacy of the means at its service becomes decisive, as Herbert A. Simon has indicated concerning the good administrative behaviour and its connection with efficiency,[31] which had been earlier associated with the notion of good administration and its correct operation[32] by the Italian doctrine. On the other hand,

[22] G. Dumont, *La citoyenneté administrative*, 666.

[23] For further development on this point see: E.Mª. Menéndez Sebastián, *De la función consultiva clásica a la buena administración. Evolución en el Estado Social y Democrático de Derecho*.

[24] Highlighting article 41 of the European Union Charter of Fundamental Rights. This has been developed in E.Mª. Menéndez Sebastián, *La apuesta europea por una buena administración: implicaciones y estado de la cuestión*, in Mª.P. Andrés Saénz De Santa María (ed.), *Una contribución a la europeización de la ciencia jurídica*: *Estudios sobre la Unión Europea*, Navarra, Thomson Reuters-Civitas, 2019, 613.

[25] In spite of the genuine endeavour made by some authors such as R. Bousta, *Essai sur la notion de bonne administration en Droit public*, Paris, L'Harmattan, 2010. Regarding the topic of *good administration,* we must also mention the multiple works by J. Ponce Solé, *Deber de buena administración y derecho al procedimiento administrativo debido. Las bases constitucionales del procedimiento administrativo y del ejercicio de la discrecionalidad*, Valladolid, Lex Nova, 2001; Id., *La lucha por el buen gobierno y el derecho a una buena administración mediante el estándar jurídico de diligencia debida*, Madrid, Cuadernos de la Cátedra de Democracia y Derechos Humanos, 2019.

[26] From Judgment of the Court of 11 February 1955, *Industrie Siderurgiche Associate (ISA) v High Authority of the European Coal and Steel Community*, case 4-54, ECLI:EU:C:1955:3, to Judgment of the Court (First Chamber) of 25 June 2020, case C-730/18 P, *SC v Eulex Kosovo*, ECLI:EU:C:2020:505, among several others.

[27] Regarding the prominent labour of this body on good administration see for example, B. Ferrer Jeffrey, *Presente y futuro del Defensor del Pueblo Europeo, guardián de la buena administración*, in *Revista de Derecho de la Unión Europea*, vol. 3, 2002, 341.

[28] Highlighting in this regard the thesis proposed by E. Chevalier, *Bonne administration et Union européennne*, Bruxelles, Bruylant, 2014.

[29] R. Bousta, *Essai sur la notion de bonne administration en Droit public.*

[30] For example, as established by article 103 of the Spanish Constitution.

[31] H.A. Simon, *Administrative behavior: a study of decision making processes in administrative organizations*, New York, NY, The Free Press, 1957, 38.

[32] Article 97 of the Italian Constitution refers to this. For instance, according to S. Cassese, *Il diritto alla buona amministrazione*, in *Relazione alla 'Giornata sul diritto alla buona amministrazione' per il 25° anniversario della legge sul 'Síndic de Greuges' della Catalogna*, Barcelona, 2009, 3, this constitutional precept entails the saction of the principles of impartiality and *good administration*.

however, it is essential to bear in mind the essence of Administrative Law, namely the balance between the public interest and particular interests.

In conclusion, the term *good administration* is used here to refer to that which serves its function well, acting without detriment to particular interests and with respect towards them. The *good administration* is such that adequately ponders current means, circumstances, facts, and evidence in order to adopt the best decision possible, for which the appropriate procedure is fundamental. The appropriate procedure fulfils two relevant functions – it contributes to better decision-making, and it stands as a guarantee of the rights of the concerned parties. This is connected with the statement of reasons, the obligation of *due care* or *due diligence* referred to by the Court of Justice of the European Union,[33] which constitutes the basis of equity.

It is also relevant to understand that the approach adopted in the proposed notion of *good administration* addresses better decision-making, better functioning, etc., from a technical-legal lens rather than a political perspective. Therefore, the proposed differentiation between *good government* and *good administration* does not only – or even primarily – refers to the subject from which the act emanates or to the rule or legal product in question. On the contrary, it addresses its character, whether technical-legal or political.

Hence, following this more or less concrete concept, the specific qualities of *good administration* ought to be considered too. This point refers to how this notion can contribute with more than just a rhetorical recognition of preexisting rights and principles, both before the administrative act and after it, concerning its control. Among these features, it is possible to highlight four: the proper functioning of the Public Administration, including the importance of standards and soft law; good administrative decision, including discretionary power, due diligence, balancing of interests, statement of reasons, assessment of facts and circumstances, etc.; a more comprehensive control, including the question of whether the legal opportunity has somehow become part of the review of legality process, which is not only judicial but also conducted by other agents such as the Ombudsperson, who plays a crucial role in this regard; and the principle of effective administrative protection understood as more than a set of procedural rights, which, according to the Spanish Supreme Court, does not end with the mere strict observance of procedure and formalities.

The necessity or advantage of connecting the notion of *good administration* – in the terms outlined here – and *administrative citizenship* is highlighted by the fact that the Charter of Fundamental Rights of the European Union, in its chapter dedicated to citizenship – articles 39 to 46 –, includes not only the right to vote and to stand as a candidate, freedom of movement and residence and diplomatic and consular protection but also the right to good administration, the right of access to documents, the European Ombudsman and the right to petition.

In addition, the connection between the aforementioned *deliberative administration* and *good administration* is apparent. The aim is to respond to the need for a transparent and open Administration facilitating the acceptability of decisions, as well as for a more efficient Administration capable of providing faster and more direct responses to the needs expressed by the citizens.[34] Moreover, if deliberation entails considering all the aspects of a phenomenon to make the right decision on the matter, it is connected with the idea of *good administration*, this is, pursuing the best possible decision by taking into account all the elements present.

In order to respond to the need for a *good administration*, even if this is understood from a restrictive perspective connected with efficiency and effectiveness only, it is undoubtedly essential to consider all the relevant viewpoints that allow making the best possible decisions. For instance, the points of view of public service users and citizens in general are crucial, and taking them into account is linked to the so-called people-based design. The needs addressed by these services must be considered to provide a better response, making the Public Administration

[33] See, for instance, the Judgment of the European Court of Justice of 4 April 2017, case C-337/15 P, ECLI:EU:C:2017:256; or the Judgement of 22 November 2017, case C-691/15 P, ECLI:EU:C:2017:882.

[34] As it has been stated by the Conseil d'État, *Consulter autrement, participer effectivement*, 92.

more effective and legitimate and even achieving greater acceptance of its decisions.

Furthermore, this notion of *administrative citizenship* integrates public consultation in the decision-making process and responds to the consideration of the user, subject, or interested party as a citizen. By acknowledging that the Administration subject is also a citizen, the civic dimension of the administrative relationship is recognised. With this transformation, the administrative relationship becomes one of the means of access to citizenship, which entails that citizens have the right to know the Administration – transparency –, to be engaged in administrative action – participation – and that the Administration must be accountable to them – accountability –. The compliance with this will lead to a more effective and efficient Administration – which is connected with the goal of *good administration* – as well as greater legitimacy.[35]

4. *Employment of algorithms in administrative decision-making*

After providing a brief explanation of the proposed notion of *good administration*, it is evident that there is a connection between this and the idea of better decision-making, optimising resources, and, in general, effectiveness and efficiency. This section will hence focus on the use of algorithms for this purpose.

In the first place, it is necessary to distinguish between digitisation, automation, and artificial intelligence. As some authors have indicated,[36] digitalisation involves the use of information and communications technology (ICT) for administrative processes, replacing paper. Automation[37] goes beyond digitisation by replacing the human operator, which requires[38] prior regulatory provisions per article 41 of Law 1 October 2015, no. 40, of Legal Regime of the Public Sector[39] (Spain). Moreover, it is common to refer to artificial intelligence concerning tasks that previously required human intervention, including the elaboration of the whole or part of the content of an administrative decision. Thus, there is artificial intelligence when it is possible to go beyond the application of the rules that the programmer has set for the algorithmic analysis of a large amount of data, and the programme creates new rules from the correlations that it discovers within the supplied data.[40]

Furthermore, setting aside the compelling debate concerning the legal nature of algorithms,[41] it should be noted that there are several types. The function of a number of them is merely to facilitate the Administration decision-making process hence they may be regarded as more elementary; for instance, programmes employed to apply a scale or formula, which could be hand-made, making it feasible to assess its correct application. Moreover, some algorithms mechanize or automate regulated processes with some degree of complexity that can be hardly replicated by human beings. Finally, perhaps the most controversial issue is predictive algorithms, which add their own decisional elements from the analysis of previous data. Thus, as the French *Défenseur des droits* has

[35] The link between both concepts has also been indicated by some authors, such as F. Delpérée, *Rapport de synthèse sur la citoyenneté administrative*, in *Annuaire européen d'administration publique*, Aix-en-Provence, Presses Universitaires d'Aix-Marseille, 2020, 205, who claims that *good administration* is a necessary condition for good citizenship.

[36] A. Huergo Lora, *Regular la inteligencia artificial (en Derecho Administrativo)*, in *Blog de la Revista de Derecho Público*, 8 March 2021.

[37] Regarding the recent use of automation by Public Administrations, see A. Cerrillo Martínez, *Robots, asistentes virtuales y automatización de las administraciones públicas*, in *Revista Gallega de Administración Pública*, vol. 61, 2021, 271.

[38] Since laws confer the power to issue administrative acts to administrative agencies, whose incumbents are natural persons.

[39] Regarding the regulation of automatised administrative operations, it is relevant to highlight the pioneer work by I. Martín Delgado, *Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada*, in *Revista de Administración Pública*, vol. 180, 2009.

[40] See A. Huergo Lora, *Regular la inteligencia artificial (en Derecho Administrativo),* who mentions the case of programmes that predict where infringements are most likely to occur based on the analysis of past transgressions within a sector, allowing the Administration to concentrate its inspection efforts there.

[41] It is relevant to briefly mention two doctrinal trends on this point - some authors consider algorithms as acts, for instance, A. Huergo Lora, *Regular la inteligencia artificial (en Derecho Administrativo),* whereas others understand that these have a regulatory nature, such as 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 decisiones*, in *Revista de Derecho Público: Teoría y Método*, vol. 1, 2020, 223.

pointed out, algorithms vary according to their conception and capacity to learn, as well as their intended prediction of events, behaviours, or individual preferences.[42]

To sum up, it is important to consider that this phenomenon represents a passage from the logical-deductive procedure to the Boolean logic of correlations and probabilities, which involves certain risks, both in the design and data.[43] This is the case with algorithms capable of learning, which can draw their conclusions and/or generate their own instructions from the available data and previous repetitions. In these cases, it is difficult to determine the reasons for the decision-making, as they are not introduced from the beginning but generated by the algorithm instead.

Nevertheless, it is also true that algorithms in particular, and artificial intelligence in general, can also contribute to better decision-making by being able to handle amounts of data that would otherwise be unattainable for humans. If employed correctly, this could contribute to a more efficient allocation of resources, hence to *good administration.*[44]

5. *Algorithmic bias and gender-sensitive*

So far it has been explained what is meant by *good administration* and which is the expected role of artificial intelligence, in particular algorithms, in it. Therefore, this section will focus on how gender equality can be affected by this new instrument in the hands of Public Administrations, as well as at the private level, and the measures that can be implemented in this regard.

There are various and several risks and benefits[45] that have been pointed out from different approaches, in terms of the digital world in general and concerning the use of artificial intelligence in particular. It is necessary to consider that the use of these technologies has not been associated in vain with the idea of effectiveness and efficiency and, hence, *good administration*.

Among the risks these may pose, it is possible to mention ethical concerns regarding *posthumanism* and the enhanced human,[46] the three levels of the digital divide, in particular, the third in terms of participation in social and political life – in the era of open government [47]-, and the gender biases of algorithms which is the specific point that this work addresses.

Even though it may be thought that algorithms would not include gender biases or discriminate, some experiences have shown the contrary.[48] For instance, it is worth mentioning a study from the University of Boston[49] which makes evident that automatic learning techniques to train an artificial intelligence system using Google news solved the analogy "man is to computer programmer, what woman is to X" with the answer to X being equal to housewife.

Another example of this issue has been pointed out in the study "Semantics derived automatically from language corpora necessarily contain human biases".[50] In this case, an algorithm trained with texts taken from the internet associated female names like Sarah with words linked to family, such as parents and wedding. In contrast, male names

[42] Défenseur des Droits, *Rapport Dématérialisation d'acces aux services publics*, Paris, 2019, 65.

[43] As stated by C. Baz Lomba, *Los algoritmos en la toma de decisiones administrativas*, in *CEF-Legal*, vol. 243, April 2021, 129.

[44] P. Padilla Ruiz, *Inteligencia artificial y Administración Pública*, in *El Consultor de los Ayuntamientos*, vol. 10, 2019, 96, follows this argument, stating that if the aim is to improve the lives of citizens and be more efficient and proactive, saving costs and time, there is no doubt that algorithms and robots should occupy a prominent place in the procedures of any Public Administration.

[45] There are authors that argue that algorithmic decisions are less biased than those made by human beings. This is the case of A.P. Miller., *Want Less-Biased Decisions? Use Algorithms*, in *Harward Business Review*, 26 July 2018.

[46] Regarding this compelling issue it is essential to refer to the work of S. Rodotà, *Diritto, scienza, tecnologia: modelli e scelte di regolamentazione*, Turin, Giappichelli, 2004, 397; as well as the following work: *Del ser humano al posthumano*, in T. De La Quadra-Salcedo and J. L. Piñar Mañas (eds.), M. Barrio Andrés M. and J. Toirregrosa Vázquez (coords.), *Sociedad digital*, Madrid, BOE, 2018, 87.

[47] For further references about the digital divide, see E. Mª. Menéndez Sebastián and J. Ballina Díaz, *Digital citizenship: fighting the digital divide*, in *European Review of Digital Administration & Law (Erdal)*, vol. 2, No. 1, 2021.

[48] As it has been explained by S. Leavy, *Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning*, in *GE '18: Proceedings of the 1st International Workshop on Gender Equality in Software Engineering*, Gothenburg, Sweden, May 2018, 14.

[49] Conducted by T. Bolukbasi, K.W. Chang, J.Y. Zou, V. Saligrama and A. T. Kalai, *Man is to computer programmer as woman is to homemaker? debiasing word embeddings*, in *Advances in neural information processing systems,* 2016, 4349.

[50] By A. Caliskan, J.J. Bryson and A. Narayanan, in *Science,* 14 April 2017, vol. 356, No. 6334, 183.

like John had stronger associations with words attributed to work, such as professional and salary.

It is also worth remembering the algorithm used by Amazon for the selection of its personnel, which had to be discarded because it showed strong gender biases, penalising resumes that contained the word "woman".

Another research has demonstrated that Bing retrieves pictures of women more frequently when the searches include words considered "warm" such as sensitive or emotional. Conversely, words referring to traits associated with "competence" such as intelligent or rational, tend to be represented by pictures of men. Furthermore, when searching for the word "person", the engine often retrieves more pictures of men than women.[51]

The paper "Balanced Datasets Are Not Enough: Estimating and Mitigating Gender Bias in Deep Image Representations"[52] has found that the algorithm would associate pictures of shopping and kitchens with women. Hence, most of the time, it would deduce that "if she is in the kitchen, she is a woman". Instead, it would associate images of physical training with men.

In addition to text data and images, user inputs and interactions also reinforce and contribute to the learning of biases by algorithms. The work "*It's a Man's Wikipedia? Assessing Gender Inequality in an Online Encyclopedia*"[53] has noted that issues related to family and romantic relationships are discussed much more frequently in Wikipedia articles on women than men. In addition, women's biographies tend to be more associated (through links) with men than vice versa.

An even clearer case of algorithmic bias can be found in gendered languages, as revealed by the study "*Examining Gender Bias in Languages with Grammatical Gender*".[54] This research showed gender biases when translating from English to languages with grammatical gender, such as Spanish and French. For example, when the word lawyer was translated from English into Spanish, there was a stronger automatic association with *abogado* (masculine) than *abogada* (feminine). On the contrary, the word nurse was more frequently related to *enfermera* (feminine) than *enfermero* (masculine). In principle, it should have associated both terms with identical probability. Despite the numerous criticisms of recent years, the biases that occur when translating from a language without grammatical gender, such as English, to a language with grammatical gender, such as Spanish or French, are still present nowadays in some automatic translators.

There are also examples in the public sector,[55] such as the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)[56] and PREDPOL cases, in the area of crime prediction, where algorithms were found to discriminate from a racial perspective.[57] It is also worth mentioning the case of BOSCO, regarding the electricity social bond in Spain, *Aadhaar* for social welfare in India, *AMS* regarding Austrian public system to detect probabilities

[51] J. Otternacher, J. Bates and P. D. Clough, *Competent Men and Warm Women: Gender Stereotypes and Backlash in Image Search Results*, in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems,* Colorado Convention Center, Denver, CO, 2017, 6620.

[52] By T. Wang, J. Zhao, M. Yatskarm, K-W. Chang and V. Ordonez, from the University of Virginia, University of California Los Angeles and Allen Institute for Artificial Intelligence, available at https://openaccess.thecvf.com/content_ICCV_2019/papers/Wang_Balanced_Datasets_Are_Not_Enough_Estimating_and_Mitigating_Gender_Bias_ICCV_2019_paper.pdf.

[53] C. Wagner, D. Garcia, M. Jadidi, and M. Strohmaier, *It's a Man's Wikipedia? Assessing Gender Inequality in an Online Encyclopedia*, in *16th International Conference on Web and Social Media*, vol. 9, No. 1, 454.

[54] This research has been conducted by P. Zhou, W. Shi, J. Zhao, K-H. Huang, M. Chen, R. Cotterell, K-W. Chang, published in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing*, Hong Kong, 2019, 5276.

[55] As it has been pointed out by P. Rivas Vallejo, *Discriminación algorítmica: detección, prevención y tutela*, in *XXXI Jornades Catalanes de Dret Social ("Treball, discriminación i Covid")*, Barcelona, April 2021, 11.

[56] www.northpointeinc.com/files/downloads/FAQ_Document.pdf. The discriminatory nature of this case, which referred to the probability of recidivism in the commission of crimes, was revealed in the report by J. Angwin, J. Larson, S. Mattus and L. Kirchner, *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks*, published on 23 May 2016 and available at www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[57] Regarding this case, see M. González, *¿Cómo funciona Predpol, el software que dice predecir dónde van a suceder crímenes?*, in *Xataka*, 14 February 2015, available at https://www.xataka.com/aplicaciones/como-funciona-predpol-el-software-que-dice-predecir-donde-van-a-suceder-crimenes.

of finding employment,[58] *System Risk Indication* (*SyRI*) in The Netherlands in terms of detection of tax and tax rate fraud,[59] among others.[60]

The risk that algorithms may discriminate is less acceptable when it comes to Public Administration, which leads to two issues. In the first place, the need to control the use of algorithms that discriminate in the private sphere relies on the Administration as the public authority entrusted by the Spanish Constitution to ensure material and effective equality and remove the obstacles that prevent it. Moreover, the Administration ought to be extremely cautious when employing these instruments in administrative decision-making, which does not mean that their use is prohibited but rather that special measures are required. This is a particularly relevant issue that needs to be addressed, considering the cases aforementioned – even though not all of them entailed discrimination from a gender perspective –, as well as the doubts and the debate surrounding the transparency of algorithms versus motivation and effective judicial and administrative protection.

The importance of an adequate use of algorithms and the need to introduce precautions in this respect seems to be addressed by the regulation draft of the European Union on new rules for Artificial Intelligence and algorithms. This regulatory framework includes a set of criteria for algorithms and corresponding risk categories.[61] In particular, this proposal for regulation at the European level establishes different scenarios: cases in which the employment of artificial intelligence – although not identical to algorithms-[62] is prohibited, cases in which this is subject to prior authorisation,[63] cases with specific provisions,[64] high-risk cases that require prior verification by a third party,[65] and other cases for which a form of prior declaration or commitment of compliance is sufficient.[66]

In conclusion, regulating the use of algorithms by Public Administrations is extremely urgent, and it is necessary to introduce precautions to avoid potential gender biases, as well as other forms of discrimination. In this line, the European Commission has adopted an anthropocentric approach in the Communication on "Building Trust in Human-Centric Artificial Intelligence" (COM/2019/168 final) and the "White paper on Artificial Intelligence - A European approach to excellence and trust" (COM/2020/65 final),[67] where ethics plays a crucial role.[68] If regaining citizens' trust in public institutions is one of the main

[58] On this regard see C. Castillo, *Algorithmic Discrimination*, in *Conference in BCN Analytics Data and Ethics event*, April 2018, available at https://youtu.be/VIl8YWWD81U?t=18m42s, and W. Fröhlich, I. Spiecker and G. Döhmann, *Können Algorithmen diskriminieren?*, in *Verfassungsblog*, 26 December 2018, available at https://verfassungsblog.de/koennen-algorithmen-diskriminieren.

[59] On this case, see the sentence by The Hague Tribunal from 5 February 2020, ECLI:NL:RBDHA:2020:1878.

[60] As highlighted by the *Défenseur des droits* in collaboration with the *Commission Nationale Informatiques & Libertés (CNIL*), *Algorithmes: prévenir l'automatisation des discriminations*, Paris, 2020, 3, nowadays these processes can be found in essential areas, such as access to social benefits, police and justice, the functioning of organisations such as hospitals, access to public services or recruitment procedures.

[61] In this regard, see A. Huergo Lora, *El proyecto de Reglamento sobre la Inteligencia Artificial*, in *Almacén de Derecho*, 17 April 2021.

[62] According to the European Ethical Charter on the use of AI in the judicial systems and their environment from 4 December 2018, an algorithm is the finite sequence of formal rules (logical operations and instructions) that allow to obtain a result of the initial input of information. This sequence can be part of an automated execution process and take advantage of models designed through machine learning; while artificial intelligence is a set of scientific methods, theories and techniques whose aim is to reproduce, through a machine, the cognitive abilities of human beings.

[63] This group includes, for example, remote biometric identification in public spaces, which is subject to administrative authorisation and will only be granted when there is a rule that allows it in order to fight against grave crimes and being subject to strict limits and guarantees.

[64] Certain applications, such as the so-called "chatbot" or the "deep fake", as well as applications of high-risk artificial intelligence, have various control mechanisms, which are listed in Annex II and regulated in articles 5-40.

[65] Such as those used for biometric identification and for the operation of critical infrastructures.

[66] The other group that does not require such independent verification but will be subjected to a form of declaration of responsibility includes typical artificial intelligence "predictive" applications. However, considering that these may still engage in discriminatory practices, other types of prior control may be appropriate.

[67] From 19 February 2020.

[68] With regard to this topic, see L. Ireni-Saban and M. Sherman, *Ethical Governance of Artificial Intelligence in the Public Sector*, London, Routledge, 2021, which argues that ethical evaluation of AI should be an integral part of public service ethics and that an effective regulatory framework is needed to provide ethical and evaluation principles for decision-making in the public sphere at both local and international levels.

objectives of the idea of new public governance, the emergence of inequalities will be a hindrance. The reason for this is that, as prior works have discussed, distrust originates in great measure from the sense of inequality.[69] Therefore, it is necessary to prevent the deepening of pre-existing differences that appear intolerable by the use of artificial intelligence since this would undermine and harm a genuine notion of citizenship.[70]

Other legal documents take into consideration the need for protection against potential algorithmic discrimination and indicate various solutions, emphasising preventive controls. Some countries have begun to adopt legal measures in their jurisdictions. For example, the United Kingdom has approved the "Guide to the General Data Protection Regulation (GDPR)",[71] which is based on the "Guide to Data Protection";[72] the United States has the "Algorithmic Accountability Act";[73] France has a general regulation on this subject in the *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*,[74] as well as the work conducted by *Etalab*,[75] including the elaboration of the *Guide d'ouverture des codes sources publics: guide pratique*;[76] Canada has made significant advances in this field with guidance on how to use algorithms ethically; The Netherlands has a tool to make algorithms available openly; New Zealand Algorithm Charter for citizens to understand how the government uses personal data.

Another relevant legal instrument is the "Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems" from 2018,[77] which aims at establishing a sort of Public Algorithms Authority; as well as the "Principles for Accountable Algorithms and a Social Impact Statement for Algorithms"[78] from the FAT,[79] among others.

From another perspective, it is also worth mentioning that the European network of legal experts in gender equality and non-discrimination has proposed a system called "PROTECT",[80] the acronym equivalent to prevent, redress, open, train, explain, control, and test, which entails seven key actions to address algorithmic discrimination; or the "2019 Artificial Intelligence for Europe document from the European Economic and Social Committee"; and the "2019 Ethics Guidelines for Trustworthy Artificial Intelligence", which stresses the need for AI not to be employed in a discriminatory way, but rather to use these tools to mitigate existing biases and discrimination.[81]

It is possible to draw various conclusions from a comparative analysis. In the first place, there is an evident concern for the appropriate use of artificial intelligence and, in particular, algorithms in the public decision-making process. Hence, several countries have been driven to take action in this regard and regulate the use of AI and algorithms, leading in turn to the European Union to issue various legal documents that can serve as a starting point towards a regulatory framework.[82]

[69] See E.Mª. Menéndez Sebastián and J. Ballina Díaz, *¿Qué es la ciudadanía hoy?*, in *Objetivos de desarrollo sostenible*, Navarra, Thomson Reuters, 2022.

[70] As it has been pointed out by J. Tomlison, *Justice in the Digital State. Assessing the Next Revolution in Administrative Justice*, Bristol, Policy Press, 2019, digital technologies have the potential to expand access to public services, but only if they are properly designed.

[71] Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr.

[72] Available at https://ico.org.uk/media/for-organisations/guide-to-data-protection-1-1.pdf.

[73] Available at https://www.congress.gov/bill/116th-congress/house-bill/2231/all-info.

[74] Available at www.legifrance.gouv.fr

[75] Available at https://etalab.github.io/algorithmes-publics/guide.html.

[76] The situation in France is most interesting since they understand that algorithms are a form of public action. Therefore, they are subject to accountability, there must be transparency, and the functioning and objectives pursued with algorithms must be adequately explained. Thus, in order to make fair decisions using algorithms in the French system, four conditions must be met: transparency, which requires an accurate description of the process; intelligibility, as the interested parties must be able to understand the process; loyalty, which entails using the procedure comprehensively and with precision; and equal treatment, hence, nobody can be favoured more than another person.

[77] Available at www.accessnow.org.

[78] Available at www.fatml.org.

[79] Acronym of Fairness, Accountability and Transparency in Machine Learning.

[80] J. Gerards and R. Xenidis, *Algorithmic Discrimination in Europe: Challenges and Opportunities for EU Gender Equality and Non-Discrimination Law, European network of legal experts in gender equality and non-discrimination*, European Commission, 2020, available at www.equalitylaw.eu.

[81] In particular requirement no. 5 refers to diversity, non-discrimination and equity.

[82] It is worth mentioning the *EU Strategy on Artificial Intelligence* from 2018, and the *White paper on Artificial Intelligence - A European approach to excellence and trust* from 2020.

Secondly, the training of public officers, and society in general, for the ethical use of algorithms becomes essential. In third place is the importance of avoiding discrimination in the application of previous instruments, for instance, analyses, evaluations, auditing,[83] certifications, etc.[84] Moreover, the employment of other measures, such as the prohibition of certain uses of algorithms or the requirement of prior authorisation, should not be ruled out, in line with what the European Union has proposed in the "Artificial Intelligence Act" aforementioned. Finally, transparency plays a crucial role in the use of algorithms. As it has been exposed by the French case, awareness regarding the relevance of this point is not enough; instead, it is necessary to understand its operation.[85] This consideration is essential from the perspective of accountability,[86] especially considering the obligation of reasoned decision-making imposed by our legal system, which must at least satisfy the *right to explanation*.[87]

The last point deserves an express mention since its connection with the *rights to good administration* and *effective administrative protection* is apparent. Without knowledge of the reasons behind a decision from the Public Administration, it is difficult to determine whether it is discriminatory or not, if it has been adopted accordingly, or if it complies with the applicable rules. All of this leads to the impossibility of combating discrimination appropriately, thus affecting effective legal protection.

All of the above highlights the importance of the issue of transparency and access to the source code. However, this does not guarantee the removal of the doubts concerning the possibility that the decision in question is biased since biases may come from the data itself.[88] In fact, some regulations have prohibited the use of algorithms in decision-making that entails the power of discretion, such as in Germany. In contrast, the general rule in France is the opening of source codes, which involves not only publishing but also explaining them.

Finally, some of the most controversial issues and risks of using algorithms in the field of Public Administration are transparency, motivation, and access to the source code. In order to fulfil the obligation of reasoned decision and not cause defencelessness, it is necessary to know the reasoning underlying the decision. Nevertheless, it is not yet clear from current regulations whether this condition entails granting access to the source code as the *Consejo de Transparencia y Buen Gobierno* seems to suggest.[89] Furthermore, it is worth mentioning the provisions of the *Carta de Derechos Digitales*, in particular section XVIII, which addresses the rights of citizens concerning artificial intelligence in the framework of administrative action, and expressly refers to comprehensible reasoning in paragraph 6. Similarly, it states the possibility of regulating access to the source code by law.

This issue is not simple and it would be advisable to advance toward its regulation in a clear and direct way,[90] such as in France. Some regulations of relevance to this topic are

[83] Article 41 of Law 40/2015 refers to this point regarding automatised administrative operations.

[84] For instance, New Zealand has an advisory board on data ethics, and the Dutch General Audit Chamber has investigated the use of algorithms in the public sector.

[85] "Transparency" and "explainability" are two key principles included in the OECD Council Recommendation on Artificial Intelligence from 22 May 2019.

[86] Nevertheless, the proposed rules for European Union regulation on artificial intelligence (Artificial Intelligence Act) do not require full transparency, but rather transparency that is sufficient and compatible with the fulfilment of the legal obligations of the user and the supplier (article 10), as has been indicated by A. Huergo Lora, *El proyecto de Reglamento sobre la Inteligencia Artificial*.

[87] As explained by P. Rivas Vallejo, *Discriminación algorítmica: detección, prevención y tutela*, 64.

[88] P. Rivas Vallejo, *Discriminación algorítmica: detección, prevención y tutela*, 64.

[88] S. Barocas and A.D. Selbest, *Big data's disparate impact*, in *California Law Review*, vol. 104, No. 3, June 2016, 671, state that there is neither technological magic nor mathematical neutrality: algorithms are designed by humans and based on data that mirror human practices. This way, biases may be present in all stages of system development and implementation: from the intention underlying the development of the algorithm to the development of the computer code, including the executable code, execution, context of execution, and maintenance.

[89] See resolution 701/2018 from 18 February 2019, especially regarding the issue of access to the code source in the BOSCO case aforementioned. This decision has been confirmed in court by the ruling of the Central Contentious-Administrative Court No. 8 of 30 December 2021 (PO 18/2019), considering that access to the source code could in this case fall within the limits of letters d), g), j) and k) of art. 14.1 of *Ley 19/2013 de Transparencia, acceso a la información y buen gobierno*.

[90] Regarding this point see A. Huergo Lora and G. M. Díaz González (eds.), *La regulación de los algoritmos*.

article 22 of the European General Data Protection Regulation,[91][92] and the *Ley de Contratos del Sector Público*. An important aspect to consider is intellectual property when the source code has been elaborated by a third party.[93] Hence it may be necessary to train public officers, not only in the application but also the design of algorithms, fostering their creation by the Public Administration itself.[94]

It is worth mentioning the provision recently established in art. 23 of *Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación*, which supports impact assessment as a mechanism to prevent possible discriminatory biases in the use of algorithms by public administrations in decision-making, as well as transparency in the design, implementation and interpretability of the decisions adopted by them.

6. *Conclusion*

We are witnessing an authentic disruption in our society largely due to two different but converging factors. On the one hand, the new relationship between citizens and the public power, in particular the Public Administration, and, on the other, the digital transformation.

With regard to the first, the French notion of *administrative citizenship* stands out, as it accurately reflects the parameters of the rights of all citizens to participate in the Administration and decision-making processes implemented at this level.[95] Since this contributes to better decision-making, it appears inextricably linked to the concept of *good administration* by providing a better response to society's demands and increasing the acceptability of its decisions.

Meanwhile, the digital revolution contributes to the effective realisation of this renewed citizenship by offering new tools that facilitate its exercise, although not without significant risks, such as the digital divide. There has also been an upsurge of another issue linked to new technologies in recent years, as is the use of artificial intelligence and, in particular, algorithms. Undoubtedly, this is a resource that can help in the aim of better decision-making and, therefore, the fulfilment of *good administration*, for example, by handling a quantity of data that would otherwise be impracticable.

Nonetheless, reality has shown that this is a controversial issue. Therefore, it is necessary to address its regulation and possess mechanisms capable of detecting and preventing algorithmic discrimination – such as a gender-sensitive perspective –, for instance, through auditing,[96] certifications, impact assessments, etc. Moreover, transparency and motivation are essential because, without knowledge or understanding of how decisions are made, effective judicial protection may be seriously compromised.

In conclusion, the use of algorithms in the public sector may contribute to the achievement of good administration and the effective exercise of administrative citizenship. However, this must be done adequately and prudently in order not to infringe fundamental rights by deepening intolerable pre-existing differences that only undermine and harm a genuine notion of citizenship.[97]

[91] 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.

[92] Which states that interested parties shall have the right not to be subjects of a decision based solely on automated processing, including profiling, that produces legal effects on them or significantly affects them, except for a series of provided exceptions.

[93] Article 308.1 of LCSP states that unless otherwise stipulated in the administrative clauses or in the contract document, service contracts for the purpose of developing and making available products protected by an intellectual or industrial property right shall entail the cession of that right to the contracting Administration.

[94] Although this does not prevent all difficulties, as publicising the source code can make the system more vulnerable.

[95] In the words of F. Delpérée, *Rapport de synthèse sur la citoyenneté administrative*, in *Annuaire international de justice constitutionnelle*, issue 35, 2019-2020, 202.

[96] As proposed by the report elaborated by M. Sáinz, L. Arroyo and C. Castaño, *Mujeres y digitalización. De las brechas a los algoritmos*, Madrid, Instituto de la Mujer y para la Igualdad de Oportunidades, Ministerio de Igualdad, 2020, 74.

[97] As has been indicated by J. Tomlison, *Justice in the Digital State. Assessing the Next Revolution in Administrative Justice*, digital technologies have the potential to expand access to public services, but only if they are properly designed.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 57-72
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 05

*Digital Transition of Public Administration in Italy and the Right to a Good Administration: Problems and Prospects Also in the Perspective of the Implementation of the National Recovery and Resilience Plan**

Diana-Urania Galetta
(Full Professor of Administrative Law at Università degli Studi di Milano)

ABSTRACT After considering the steps needed to reach the goal of digitalizing public administration, the paper aims to verify whether and to what extent a public administration that makes use of ICT is (or could be) a better public administration in the sense of better responding to that right to a good administration referred to in art. 41 of the Charter of Fundamental Rights of the European Union and what role the National Recovery and Resilience Plan could play in this perspective.

1. *Introductory remarks*

In order to be able to address the question of what challenges are imposed on public administration today by the so-called digital transition, it is first necessary to have a clear idea of what "digital transition" means and what steps it actually entails for our public administrations.

Summing up here what I have discussed in greater detail elsewhere, digital transition implies the use of Information and Communication Technologies (ICT) within public administrations, with the aim of providing services that meet the needs expressed by citizens in a society that has changed profoundly especially thanks to the use of such technologies.[1]

As it was already explicitly stated in the 2003 EU Commission Communication on the role of eGovernment for Europe's future "Information and communication technologies (ICT) can help public administrations to cope with the many challenges. However, the focus should not be on ICT itself. Instead it should be on the use of ICT combined with organisational change and new skills in order to improve public services, democratic processes and public policies. This is what eGovernment is about".[2]

This means that the digital transition is not (and should not be conceived) as an end in itself, to be achieved "whatever it takes". ICT are to be seen as a useful means to an end, which clearly needs to be identified in advance.

The introduction of ICT in the context of administrative procedures must serve, first of all, the objective of making public administrations more efficient, improving on the one hand the quality of public services provided to citizens and, on the other hand, reducing the related costs for the community, at least in a medium to long term perspective.[3] With this in mind, the reference model is that of *e-commerce,* whose essential value is, precisely, its efficiency.[4]

The introduction of ICT is therefore seen as being closely related to the objective of modernising public administration: ensuring greater efficiency, but also transparency and

* Article submitted to double-blind peer review.
The article was drafted in view of its publication in the book in honor of Patrick J. Birkinshaw (Kluwer Law International, 2023).

[1] See D.U. Galetta, *Information and Communication Technology and Public Administration: through the Looking-Glass*, in D.U. Galetta, J. Ziller (eds.), *Information and Communication Technologies Challenging Public Law, beyond Data Protection*, Baden-Baden, Nomos Verlagsgesellschaft, 2018, 119.

[2] See Commission Communication of 26 September 2003, The role of eGovernment for Europe's Future, Doc. COM(2003) 567 final, at *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0567:FIN:EN:PDF*, 4.

[3] See W. Sheridan, T.B. Riley, *Comparing e-Government vs. e-Governance*, in *Geospatial World*, 2010, 1.

[4] Among others: C. Zotta, R. Amit and J. Donlevya, *Strategies for value creation in e-commerce: best practice in Europe*, in *European Management Journal*, vol. 5, 2000, 463.

simplification of its activities and, consequently, improving the quality of relations with citizens, as well as the service provided to them.[5]

In the perspective of this paper, however, the aim identified as an objective would be that of guaranteeing a better satisfaction/realisation of that right to good administration whose reference parameter is Article 41 of the Charter of Fundamental Rights of the European Union. With this in mind, it is necessary to verify whether and to what extent a public administration that makes use of ICT is (or can be) a better public administration in the sense of being more compliant with the canons of good administration codified therein.

In order to do this, it is obviously necessary to examine - also on the basis of concrete examples - the various and numerous problems and critical issues linked to the so-called digital transition of public administration.

2. *The digital transition of public administration: the necessary steps and related issues*

2.1. *The dematerialisation of documents held by public administrations*

In order to be able to identify the potentialities and problematic issues related to the use of ICT in the context of public administration, it is first of all necessary to clarify - albeit quickly - the fundamental steps to be taken in order to achieve the so-called "digital transition".

The very concept of transition (from the Latin *transire*, i.e. "to pass") identifies "a change or shift from one state, subject, place, etc. to another".[6] Therefore, once this transition has been completed, one should, in theory, find oneself before a new and different (better?) public administration than the one from which one started.

The first step of this transition, however, already implies an enormous amount of work, which consists in transforming traditional paper documents and archives into electronic documents and archives;[7] and in abandoning, for the future, the production of "paper native" documents and opting instead for "digital native"[8] documents.

Dematerialisation is, in fact, a *conditio sine qua non* to be able to improve efficiency and control of documents, easy sharing of documents and data, storage and security of information, allowing (at least in perspective) savings in time and resources.

Digital files are considered better than traditional paper documents (or those anchored to a physical medium) insofar as they do not take up "physical" space in offices, can be easily retrieved and copied, and individual contents can be extracted much more efficiently than from paper documents.

However, this is only true in principle. As the complex story of the creation of the National Register of Resident Population (*Anagrafe Nazionale della Popolazione Residente* - ANPR) in Italy clearly shows: the national database into which all the 7,903 municipal registers have gradually converged since 21 October 2016.[9]

Even more so, as to the creation of the Electronic Health Record (*Fascicolo Sanitario Elettronico* - FSE).[10] According to Article 12, para 1 of Decree-Law 179/2012, the EHR is "the set of data and digital documents of a health and social-health nature generated by present and past clinical events concerning the patient, also referring to services provided outside the National Health Service".[11]

Apart from the specific problems related to the content of the EHR and its concrete implementation,[12] (*infra,* par. 4.2.), if one

[5] On this point see D.U. Galetta, *Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens?*, in *European Public Law*, vol. 25, issue 2, 2019, 171.

[6] See at www.merriam-webster.com/dictionary/transition.

[7] See S. Armenia, D. Canini and N. Casalino, *A system dynamics approach to the Paper Dematerialization Process in the Italian Public Administration*, in D'Atri et al. (eds.) *Interdisciplinary Aspects of Information Systems Studies*, Heidelberg, Physica-Verlag, 2008, 399.

[8] That is, obtained using word processing software and transformed directly into PDF (and not by scanning a paper document).

[9] At 31 December 2021, only the municipality of San Teodoro, in the province of Messina, was still missing. See *infra*, para 4.2.

[10] See M. Moruzzi, *La sanità dematerializzata e il fascicolo sanitario elettronico. Il nuovo welfare a "bassa burocrazia"*, Rome, Il Pensiero Scientifico, 2014.

[11] Decree-Law 179/2012, converted with amendments by Law no. 221 of 17 December 2012 (in Official Gazette no. 208 of 18 December 2012, no. 294). All translations from Italian (or other languages) into English contained in this paper are mine and therefore solely my responsibility.

[12] See R. Ducato and P. Guarda, *From electronic health records to personal health records: emerging legal*

considers the way in which most of the information contained in citizens Electronic Health Records was initially transferred from a paper file to an electronic one, one finds out that this is in itself an obstacle in achieving the objective of immediate availability of relevant patient information. Dematerialisation has in fact mostly been achieved, at least in the first phase, through the mere scanning of paper documents, which are then converted into non-indexable[13] pdf files. Whereas, in order to allow a real usability of the information contained in the EHF, the indexing of the files certainly represents an essential step.

2.2. *The creation and necessary maintenance of digital documents and archives*

Even if, with a burst of optimism, one would disregard the problems linked to the dematerialisation of documents mentioned above and imagine a public administration that - having successfully completed the transition to a full and complete dematerialisation of the documents in its possession - has happily moved from paper to digital documents, the problems would still not be over.

If public administrations were capable of producing only truly digital documents (i.e. not merely scanning paper documents), one could eliminate paper archives and mitigate the problems related to the managing of "physical space" in public offices.[14]

However, computer archivists[15] warn us that digital archives also have their own specific (and relevant) problems. The continually ongoing process of technological change threatens management and maintenance of digital records.

The resulting problems are obviously many and not insignificant. They concern both the accessibility over time of the contents of the digital document and the integrity of the documents themselves,[16] which are in fact much more vulnerable than classic paper documents.[17]

To mention just a few of the critical situations that may arise:[18] the software that originally could read the file format may no longer exist; the medium on which the file was stored may be lost or destroyed. This explains the meaning of the discussion about the need for public administrations[19] to "move to the cloud": a move that is, however, neither simple nor risk-free.[20]

In addition to this, an enormous problem is that the data contained in electronic documents are not physically "attached" to their media (as ink is to paper documents).

For analogical "documentary sources" the passing of time determines, at least in principle, that they remain largely unaltered, so that it is possible to ensure the conditions for verifying authenticity (e.g. by analysing the support, the writing materials, the structure of the document, the type of annotations

issues in the Italian regulation of e-health, in *International Review of Law, Computers & Technology*, vol. 9, 2016, 271.

[13] An "image" PDF whose text will not be "searchable" unless OCR software is used to scan it (to detect text within a digital image), resulting in an optical character recognition process.

[14] To give just one example of such problems: for Italy Ministerial Decree 9/3/2007 sets a number of limits on the total amount of paper that can be stored per unit of space in order not to incur a high fire risk. See the document at the link: *www.vigilfuoco.it/allegati/PI/DisposizioniGeneraliPI/COORD_DM_09_03_2007-DM_16_02_2007_RESISTENZA_AL_FUOCO.pdf*

[15] See in particular M. Guercio, *Archivistica informatica. I documenti in ambiente digitale*, Rome, Carocci, 2002.

[16] M. Guercio, *Archivi digitali. Principi, metodi e criticità organizzative*, in *Treccani*, *www.treccani.it/enciclopedia/archivi-digitali_%28XXI-Secolo%29.*

[17] See D. Bearman, *Reality and Chimeras in the Preservation of Electronic Records*, *D-Lib Magazine*, 1999, vol. 5, no. 4; Dwivedi, *Archive - where it started and the problems of perpetuity*, in *Proceedings of the Eighteen IEEE Symposium on mass storage systems and technologies*, 2001, at http://storageconference.us/2001/papers/p10dwive.pdf, 353, which well underlines how "The new era has instigated a major change for archivists from a world of "human-readable" data to one of "computer-ciphered" data, introducing a completely new set of issues and processes" (354).

[18] In addition to those already quoted see I. Boydens, *La conservation numérique des données de gestion (Numéro spécial "Archivage et perennisation"*), vol. 8, no. 2, Paris, Hermès Sciences, 2004, 13.

[19] In this regard, the Three-year Plan for IT in public administration 2021-2023 published by AGID in October 2021 explicitly refers, among the guiding principles, to the "cloud first" principle: public administrations, when defining a new project and developing new services, adopt the cloud paradigm first, taking into account the need to prevent the risk of lock-in (para 5). See also the relevant information at *https://cloud.italia.it/.*

[20] See the 2012 AGID document, Raccomandazioni e proposte sull'utilizzo del Cloud Computing nella Pubblica Amministrazione (Recommendations and proposals on the use of cloud computing in public administration), *www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/raccomandazioni_cloud_e_pa_-_2.0_0.pdf.*

etc.).[21] On the contrary, this is not at all true for electronic documents, which can easily be modified. More attention needs therefore to be paid to the issue of their integrity, authenticity and reliability.[22]

Together with the problem of the inevitable (and rapid) obsolescence of hardware and software, this means that the "once-for-all principle" that applied to the archiving of paper documents no longer applies to the archiving of electronic data.[23] Thus, one must rather speak of an "all-the-time principle" with regard to digital archiving,[24] which implies an endless commitment, also and above all financially. Adequate financial resources have to be constantly made available in order to meet the (ordinary) costs of system administration, updating of technologies, adaptation of human resources etc. With the important consequence that, at the end of the day, digital archiving is much more vulnerable to reductions in the budgets available to public administrations for current expenditure; and it is completely incompatible with the very idea of zero "maintenance" costs.

So, it is evidently necessary to start asking already now what might happen in a post National Recovery and Resilience Plan[25] scenario. Given that the recent trend in Italy has been what I have elsewhere described as "zero-cost reforms": that is, reforms that come to life accompanied by that notorious "financial invariance clause" according to which no new or greater burdens on public finances should result from their implementation.[26]

2.3. *New "social needs" and the temptation of outsourcing (the different choice of the National Recovery and Resilience Plan - NRRP)*

Studies by sociologists studying the public administration also alert us to the fact that the use of ICT and e-governance is developing in a social environment populated by increasingly demanding "clients" (citizens, professionals and private sector companies).[27] This, in turn, implies having more financial resources to meet and satisfy these "social needs" and, therefore, greater budgets to offer services related to these new "social needs".[28] The paradox, however, is that while they are increasingly demanding as citizens in terms of the facilities and services expected from the public administration, at the same time they appear, as taxpayers, less and less willing to pay for these services.

In order to overcome the dilemma that this inevitably creates for public administrations that are constantly underfunded and increasingly overloaded with tasks and burdens, there is a strong temptation for them to turn to the private sector and outsource these "services".[29] This is particularly true in the UK and United States context; but in reality, it is a widespread phenomenon in our national administrations too, partly because of the enthusiasm about resorting to the private sector (outsourcing) that has characterised the

[21] M. Guercio, *Archivi digitali* cit.

[22] The literature on this point is as complex as it is extensive. Among the many authors see K. Stranacher, V. Krnjic, B. Zwattendorfer and T. Zefferer, *Evaluation and Assessment of Editable Signatures for Trusted and Reliable Public Sector Data*, in *Electronic Journal of e-Government*, vol. 11, no. 2, 2013, 360; M. Runardotter, C. Mörtberg and A. Mirijamdotter, *The Changing Nature of Archives: Whose Responsibility?*, in *Electronic Journal of e-Government*, vol. 9, no. 1, 2011, 68; F. Buccafurri, G. Caminiti and G. Lax, *Threats to Legal Electronic Storage: Analysis and Countermeasures*, in: K. Normann Andersen et al. (Eds.), *Electronic Government and the Information Systems Perspective* (Proceedings of the Second International Conference, EGOVIS 2011, Toulouse, France), Berlin, Heidelberg, 2011, 68.

[23] See M. Dečman, *Long-term Digital Archiving - Outsourcing or Doing it*, *The Electronic Journal of e-Government*, vol. 5, no. 2, 2007, 136.

[24] M. Dečman, *Long-term Digital Archiving - Outsourcing or Doing it.*

[25] The Italian Recovery and Resilience Plan (NextGenerationItaly), can be read at *https://www.governo.it/sites/governo.it/files/PNRR.pdf.*

[26] See on this point in D.U. Galetta, *Trasparenza e contrasto della corruzione nella pubblica amministrazione: verso un moderno panottico di Bentham?*, in *Diritto e Società*, no. 1, 2017, 43, par. 6 s. But see also in D.U. Galetta, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva in una prospettiva di diritto comparato ed europeo*, in *Rivista italiana di diritto pubblico comunitario*, no. 5, 2016, par 5.8., 1054.

[27] See S. Ho Ha and M. Jung Lee, *E-Government Services Using Customer Index Knowledge*, in K. Norman Andersen et al. (eds.), *Electronic Government and the Information System Perspective* (First International Conference, EGOVIS 2010, Bilbao, Spain, August 31 - September 2, 2010, Proceedings), Berlin, Heidelberg, 2010, 174.

[28] See H. Chesbrough, *Toward a science of services*, in *Harvard Business Review*, vol. 83, 2005, 16.

[29] See on this point M. C. Lacity and R. Hirschheim, *Information systems outsourcing; Myths, Metaphors and Reliabilities*, John Wiley & Sons Ltd, England, 1993; E. S. Savas, *Privatizing the public sector: How to shrink government*, London, Chatham House, 1982.

Italian "institutional scene"[30] for a long time, now.

However, the "outsourcing solution"[31] raises a number of critical issues, not least for the fact that it does not actually reduce public spending, while it throws "smoke and mirrors" at citizens with the idea that "shrinking" the administrative apparatus is the solution to the "costs problem".[32]

The only sure outcome, in my eyes, is that the public administration takes a step backwards from its fundamental task of guardian of the public interest. With all the related consequences.

This is true in general, but even more so where outsourcing refers to services of dematerialisation and digital archiving of public documents, with the well-known (and very important) problems of security and protection of the personal data of all those involved.

In this sense, I very much welcome the strategy outlined in the Italian Recovery and Resilience Plan,[33] which I see moving in a different direction. In fact, there are huge resources invested by the Plan for public administrations, with the aim of creating the internal "resources" - in terms of civil servants, "cutting-edge and 4.0 technologies" and training in their use - capable of allowing Italian public administrations to proceed along the path of "digital transition".

However, an important question remains in the background: what will (or could) happen about all this in a post-NRRP scenario, in which the available financial resources will necessarily be scarcer?

3. *The right to good administration and its link with the digital transition*

3.1. *The origins of the right to good administration*

In this regard, the starting premise is so obvious that, perhaps, it would not even be necessary to recall it here. As is now well known, since the adoption of the Charter of Fundamental Rights, in the context of the European Union the so-called "good administration" is characterised not only as a duty of the public administration[34] but as a new fundamental right of the individual[35]: the right to good administration, as written and detailed in Article 41 of the EU Charter.[36]

Its legal notion coincides with the philosophical idea best expressed by the Iberian philosopher *Rodríguez-Arana* who underlines that "A good public administration is one that objectively serves the citizenry (...), that carries out its work rationally, justifying its actions and that is continuously oriented towards the general interest. A general interest which, in the social and democratic State governed by the rule of law, lies in the permanent and integral improvement of people's living conditions".[37]

I believe that this approach can be shared by all, whatever the concept of "improving living conditions" may be and regardless of one's political/ideological orientation.

In other words, I believe that there can be a "common understanding" among public administration scholars on this basic idea.

As to the concrete content of the provision of the EU Charter, according to Article 41(2), the right to good administration includes in particular:

1. the right of every individual to be heard before an individual measure adversely affecting him or her is taken;
2. the right of access to his/her file;
3. the obligation of the administration to

[30] As for Italy, paradigmatic in this respect is the 2013 document to be found on the website of the Presidency of the Council of Ministers, Department of the Civil Service, at *http://qualitapa.gov.it/sitoarcheologico/relazioni-con-i-cittadini/utilizzare-gli-strumenti/outsourcing/index.html*.

[31] Outsourcing is the contraction for "outside resourcing".

[32] See J. A. O'Looney, *Outsourcing State and Local Government Services: Decision-Making Strategies and Management Methods*, Quorum Books, London, 1998, 22.

[33] See at *www.governo.it/sites/governo.it/files/PNRR.pdf.*

[34] G. Falzone, *Il dovere di buona amministrazione*, Milan, Giuffrè, 1953.

[35] The first to have clearly identified it as a new fundamental right (and no longer as a mere "guiding principle" of administrative action) is A. Zito, *Il "diritto ad una buona amministrazione" nella Carta dei diritti fondamentali dell'Unione europea e nell'ordinamento interno*, in *Rivista italiana di diritto pubblico comunitario*, vol. 5, 2002, 433. See also C. Marzuoli, *Carta europea dei diritti fondamentali, "amministrazione" e soggetti di diritto: dai principi sul potere ai diritti dei soggetti*, in G. Vettori (eds.), *Carta europea e diritti dei privati,* Padua, Cedam, 2002, 255. (265).

[36] See for all: D.U. Galetta, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della pubblica amministrazione*, in *Rivista italiana di diritto pubblico comunitario*, vol. 3, 2005, 819-857.

[37] J. Rodríguez-Arana, *La buena administración como principio y como derecho fundamental in Europa*, in *Derecho y Ciencias Sociales,* vol. 6, 2013, 23, especially 26.

give reasons for its decisions.

However, this list should not be considered as exhaustive of everything that may be included in the right to good administration. The most general notion is to be found in Article 41(1) of the Charter: it is the right of every person "to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union".

The EU Court of Justice has now clearly and explicitly stated that "the right to good administration, enshrined in Article 41 of the Charter, reflects a general principle of EU law, which is applicable to Member States when they are implementing that law".[38] Moreover, for Italian law scholars Article 41 of the Charter expresses the same idea of Article 97 of the Italian Constitution, with respect to the need for impartiality and good performance of the public administration.[39]

In fact, the two provisions complement each other: an administration whose public offices are organised in such a way as to ensure good performance and impartiality is also the only one capable of guaranteeing fair and impartial treatment of matters affecting the people it administers, as required by Article 41 of the EU Charter. Similarly, an administration whose public offices are organised in such a way as to ensure good performance appears to be the only one capable of guaranteeing compliance with the "reasonable time" (for handling an affair/taking a decision) referred to in Article 41 of the EU Charter.[40] In other words, the principle of good performance certainly also encompasses a need for efficiency in public administration.[41]

3.2. *The link between the digital transition and the right to good administration and the central role of the "public officer in charge of the procedure" (responsible officer[42]).*

Turning to the specific issue at hand, the question is whether and how the use of modern Information and Communication Technologies (ICT), including algorithms[43] and Artificial Intelligence,[44] can (or cannot) contribute to the goal of "good administration".

In order to be able to provide an adequate answer to this crucial question it is necessary to bear in mind that, in Italian law, the best translation of the good administration's canons is Law 241 of 1990 on administrative procedure.[45] This law is in line with the idea expressed at the time by our best doctrine regarding the need to connect to a specific "procedure" (*proceduralizzare)* impartiality

[38] See most recently Court of Justice, judgment of 10 February 2022, in Case C-219/20, *LM*, ECLI:EU:C:2022:89, paragraph 37. See also CJEU, judgment of 24 November 2020, in joined cases C-225/19 and C-226/19, Minister of State for Foreign Affairs and Security. C-225/19 and C-226/19, Minister van Buitenlandse Zaken, ECLI:EU:C:2020:951, paragraph 34 and case-law cited therein. For further discussion on this issue see D.U. Galetta, *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art 41 della Carta dei diritti UE)*, in *Rivista italiana di diritto pubblico comunitario*, vol. 2, 2019, 165.

[39] See, among many others: P. Calandra, *Efficienza e buon andamento della pubblica amministrazione*, in *Enciclopedia Giuridica Treccani,* vol. XVIII, Rome, Istituto Enciclopedia Italiana, 2009; A. Andreani, *Il principio costituzionale di buon andamento dell'amministrazione pubblica*, Padua, Cedam, 1979.

[40] See more extensively on this point D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie TIC)*, in R. Cavallo Perin and D.U. Galetta (eds.), *Il Diritto dell'Amministrazione Pubblica digitale*, Turin, Giappichelli, 2020, 85.

[41] On this subject, see most recently S. Pignataro, *Il principio costituzionale del "buon andamento" e la riforma della pubblica amministrazione*, Bari, Cacucci editore, 2012, *passim.* See also L. Iannuccilli and A. de Tura, *Il principio di buon andamento dell'amministrazione nella giurisprudenza della corte costituzionale*, in *www.cortecostituzionale.it/documenti/convegni_seminari/STU_212.pdf*, which contains a very useful selection of fundamental rulings of the Constitutional Court in this regard.

[42] This is the expression used in the ReNEUAL Model rules. See at h*ttp://reneual.eu/projects-and-publications/reneual-1-0*. It is referred to as "responsible member of staff" in the European Parliament resolution of 9 June 2016 for an open, efficient and independent European Union administration (2016/2610(RSP)), at *www.europarl.europa.eu/doceo/document/TA-8-2016-0279_EN.pdf?redirect*.

[43] An algorithm can be defined as a precise set of instructions or rules, or a methodical series of steps that can be used to make calculations, solve problems and make decisions. See R. Benítez, G. Escudero, S. Kanaan and D. Masip Rodó, *Inteligencia artificial avanzada*, Barcelona, Editorial UOC, 2013, 14.

[44] Artificial intelligence systems use computers, algorithms and various techniques to process information and solve problems or make decisions. In this regard, it is interesting to read a recent judgment of the Italian Council of State, sec. III, 4 November 2021, no. 7891, which discusses the distinction between algorithm and Artificial Intelligence, drawing a whole series of consequences in terms of legal reasoning.

[45] For a non-official translation into English see at *www.legislationline.org/download/id/5393/file/Italy_Law_Administrative-procedure_1990_am2010_en.pdf*.

and good performance.[46] This idea has also been taken up and emphasised by our Constitutional Court[47] which, although it has never recognised the "constitutional status" to the principle of "due process" in the context of administrative procedure,[48] has however progressively overcome the negative attitude linked to concerns of reduced "functionality" of an administration tied to "excessively detailed rules of conduct".[49] And it has ended up favouring the thesis of those who linked administrative procedure to the objectives of transparency, publicity, participation and timeliness of administrative action, understood as essential values in a democratic system.[50]

At least since the beginning of the Nineties, the principles of impartiality and good performance have also been linked to the need to modernise the "administrative machinery" and to carry out an adequate reorganisation of it.[51] It is precisely in this perspective that the fundamental role that ICT can play in the context of public administration has been strongly highlighted. It is, in fact, no coincidence that the version of Article 3-bis of Law 241 on administrative procedure - as innovated by the "Simplification Decree" No. 76/2020 - provides that "In order to achieve greater efficiency in their activities, public administrations shall act by means of computer and telematic tools, in their internal relations, between the different administrations and between these and private parties".[52]

The provision - which in its current version seems to me to imply a real obligation for public administration to act "by means of computer and telematic tools"[53]- does not, however, specify in any way how and with what resources (economic and instrumental) each and every public administration would be required to implement it. Therefore, it has been identified in the doctrine as a largely useless provision, with merely programmatic content.

In addition to what I will explain later *(infra*, par. 4.) - regarding the positive impact that the NRRP may have in this context, net of the risks linked to the temporally limited duration of such resources - it appears evident to me that the provision of art. 3-bis of Law 241/90 is addressed, in the first place, to the responsible officer: in the specific perspective of his/her task of ensuring "the proper and prompt conduct" of the investigation phase of the administrative procedure; a task expressly assigned to him/her by art. 6 letter b) of the Italian Law (241/90) on administrative procedure.

I would even go so far as to say that Article 3-bis of Law 241/90, in its 2020 amended version, gives rise to a real obligation for the responsible officer to act by means of computer and telematic tools "in order to achieve greater efficiency". In particular, with a view to being able to carry out an adequate and prompt preliminary investigation in the context of the administrative procedure.

The provision of Art. 3-bis is in fact directly linked to Art. 12 of the Italian Digital Administration Code[54]: which links the use of information and communication technologies by the public administration with the aim of "autonomously organising its own activity", in order to achieve "the objectives of efficiency, effectiveness, cost-effectiveness, impartiality,

[46] See for all G. Berti, *La pubblica amministrazione come organizzazione*, Padova, Cedam, 1968, *passim.*

[47] See in particular Judgments nos. 40 and 135 of 1998.

[48] Initially denied in various judgments. See, for example, Constitutional Court, judgment no. 23 of 1978: "It should be recalled, first of all, that the so-called principle of due process (in view of which private individuals should be able to present their reasons, before measures limiting their rights are adopted) cannot be considered as constitutionalised".

[49] The Italian Constitutional Court observed in judgement no. 234 of 1985 that "with excessively detailed rules of conduct imposed on the public administration, far from always obtaining an effective guarantee, there could, on the contrary, be disadvantages, even serious ones, of stagnation".

[50] More precisely, the Constitutional Court's judgment no. 262 of 1997 states that "By means of the above-mentioned system (see Law no. 241 of 1990 and subsequent additions and, as regards the Veneto Region, see Regional Law no. 1, Chapter IV of 10 January 1996) the legislator wished to give general application to rules - largely already set out in case law and doctrine - which are the implementation, albeit not exhaustive, of the constitutional principle of good administration (art. 97 of the Constitution) in the objectives of transparency, publicity, participation and timeliness of administrative action, as essential values in a democratic system". See also Constitutional Court judgment no. 104 of 2006.

[51] See (well before that) the fundamental remarks of M. Nigro, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milan, Giuffrè, 1966, *passim*.

[52] Decree-Law no. 76 of 16 July 2020, Urgent measures for simplification and digital innovation.

[53] See already in D.U. Galetta, D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie TIC)*, 93.

[54] The Italian Digital Administration Code can be read at *www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82*.

transparency, simplification and participation". Whereas, of course, Art. 3-bis of Law 241/1990 has a field of application that clearly goes far beyond the mere scope of the internal organisation of administrative activities.

In this sense, the link with the right to good administration enshrined in the EU Charter is very clear. In the case-law it has in fact been made clear how Art. 41 of the EU Charter means in particular, that "all factual and legal information available" must be taken into consideration in such a way as "to apply due diligence in the decision-making process and to adopt its decision on the basis of all information which might have a bearing on the result".[55] This fully coincides with the need to carry out an adequate investigation in the administrative procedure, which Article 6 letter b) of Italian Law 241/90 expressly attributes as his/her task to the responsible officer. This implies, in turn, in a scenario characterised by the availability of sophisticated IC technologies, the necessity of using (also) all instruments allowing, today, the public administrations, to easily acquire not only documents, but also all that information which can be acquired through sensors and monitoring instruments of various types, which are now widely available to them.[56]

In essence, it is about "giving back" to the figure of the responsible officer the central role that it deserves, also with a view to fully exploiting its potential in this renewed scenario of digitalized administration.[57] In fact, beyond the task already attributed to him/her by art. 41 para 2 of the Italian Digital Administration Code, of preparing the so-called "electronic file",[58] there is room for the responsible officer to play a much more crucial role.

In the context of a truly digitalized public administration (the so-called public administration 4.0[59]) the responsible officer should in other words be the guarantor, first and foremost, of respect for those principles of fairness and impartiality in the investigation phase of the administrative procedure to which both Article 41 of the EU Charter and Article 97 of the Italian Constitution refer.[60]

From a practical point of view this implies that, within the framework described, he/she also takes on the task of adopting concrete organisational solutions. With the aim of avoiding discrimination between citizens on the basis of their different levels of "computer literacy" and their different availability of IT tools (and access to the network), i.e. taking on the negative consequences linked to the so-called *digital gap/digital divide*.[61]

In addition to this, it seems clear to me that, in the context of the obligation to manage administrative procedures "using information and communication technologies" established by art. 41 of the Italian Digital Administration Code, it is up to the responsible officer to break the veil of the so-called "algorithmic neutrality".[62] It is up to him/her to assess whether the possible use of Artificial Intelligence algorithms in the investigation phase of the administrative procedure, rather than favouring the objective of good administration (a fairer and more impartial decision, as well as a faster one), may instead lead to the result of discriminating - which becomes systematic, if inserted in an

[55] Judgment of the Court of First Instance (First Chamber) of 19 March 1997. Estabelecimentos Isidoro M. Oliveira SA v Commission of the European Communities, Case T-73/95, ECLI:EU:T:1997:39, point 32.

[56] In this regard, reference should be made, for example, to the document of the Italian Ministry of Public Works, General Inspectorate for Circulation and Road Safety, on the Traffic Monitoring System and in particular its appendix B, Systems and technologies for road traffic monitoring, which can be read at *https://webcache.googleusercontent.com/search?q=cache:i7TV8OuULKYJ:https://trafficlab.eu/bfd_download/linee-guida-del-monitoraggio-del-traffico/+&cd=1&hl=en&ct=clnk&gl=en&client=firefox-b-d.*

[57] See *amplius* in D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie TIC)*, 88.

[58] On which see S. D'Ancona, *Il documento informatico e il protocollo informatico*, in R. Cavallo Perin and D.U. Galetta (eds.), *Il diritto dell'amministrazione pubblica* digitale, 159, especially 187 ff.

[59] See 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 *Federalismi.it*, vol. 3, 2019, 1.

[60] See also D.U. Galetta, *Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens?*, 171.

[61] On the "digital divide", see S. D'Ancona and P. Provenzano, *Gli strumenti della Carta della cittadinanza digitale*, in R. Cavallo Perin and D. U. Galetta (eds.), *Il diritto della amministrazione pubblica digitale*, 226. See also D. Donati, *Digital divide e promozione della diffusione delle TIC*, in F. Merloni (ed.), *Introduzione all'eGovernment: pubbliche amministrazioni e società dell'informazione,* Turin, Giappichelli, 2005, 209.

[62] On which see, among many others, M. Airoldi and D. Gambetta, *On the myth of algorithmic neutrality*, in *The Lab's Quarterly*, vol. 4, 2018, 25.

algorithm![63] - between different categories of citizens.

On this last point, it should be pointed out in conclusion that, if in the context of their "power of self-organisation" it is appropriate to allow public administrations to make use of all the tools made available by ICT today, the use of such tools is conditional, first of all, on the circumstance that their use actually allows "improving the quality of services rendered to citizens and users".[64] So, if it is true - as Jean Bernard Auby recently put it - that algorithms are a way of managing complexity,[65] then it is certainly necessary for the public administration to make use of them! At the same time, however, one must be careful not to be lulled into the illusion that algorithms are the tool through which it is possible to correct the imperfections inherent in the cognitive processes and choices adopted by human beings/public officials (bias, preferences, partiality, etc.).[66] It is therefore necessary that the use of these tools brings with it a *guarantee* (and not just a vague promise!) of a more complete preliminary investigation in the administrative procedure, one which is more in keeping with the principles of impartiality and good performance; and that all this also takes place in a context of compliance with the principle of transparency.

In fact, even with regard to the so-called "robotized administrative procedures", the Italian administrative courts have not *per se* excluded the possibility of resorting to them;[67] however, what is certainly excluded is the possibility of accepting "the non-intelligibility of the operations carried out"[68] on the basis of the use of such algorithms.[69]

The principle of transparency - compliance with which the public officer responsible for the procedure must guarantee in his relationship with the addressee of the measure adopted - implies full knowledge of the existence of any automated decision-making processes and of the algorithms used[70] for that purpose.

In this framework, one must certainly move in the direction of models of *by-design* transparency and *by-default* transparency: in the logic of a digitalized administrative procedure, but which is at the same time respectful of all those principles that must govern administrative action as specified in Article 1 of Italian Law 241/90.[71] And also the right to the protection of personal data of private subjects involved in the administrative procedure plays here a very important role; therefore, one could certainly imagine to go in the direction of those principles of privacy *by design* and privacy *by default* contained in the GDPR.[72]

To conclude on this point, in the perspective of the transition towards the so-called Administration 4.0,[73] the figure of the responsible officer, far from being obsolete, seems to me to represent the essential pivotal-point in the relationship between the digitalisation of public administration and good administration. In fact, it is only thanks

[63] On this point see, among others: D. Freeman Engstrom and D. E. Ho, *Algorithmic Accountability in the Administrative State*, in *Yale Journal on Regulation*, vol. 37, no. 3, 2020, also available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3551544*; L. Ayre and J. Craner, *Algorithms: avoiding the implementation of institutional biases*, in *Public Library Quarterly*, vol. 37, no. 3, 2018, 341; K. M. Altenburger and D. E. Ho, *When Algorithms Import Private Bias into Public Enforcement: The Promise and Limitations of Statistical Debiasing Solutions*, in *Journal of Institutional and Theoretical Economics,* vol. 175, no. 1, 2018, 98; S. B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, in *Stanford Law Review*, vol. 66, no. 4, 2014, 803.

[64] Thus Cons. Stato, judgment 5 December 2019, no. 8472, point 8.1.

[65] As stated by J-B. Auby, *Il diritto amministrativo di fronte alle sfide digitali*, in *Istituzioni del Federalismo*, vol. 3, 2019 619.

[66] On cognitive biases and their consequences on choices made by public administrations see most recently S. D'Ancona, *Contributo allo studio della progettazione in materia di appalti e concessioni. Una prospettiva dalle scienze comportamentali e cognitive*, Torino, Giappichelli, 2021.

[67] See in particular Cons. Stato, judgment of 5 December 2019, no. 8472 cit.

[68] Cons. Stato, sec. VI, judgment 21 January 2021, no. 799, in *https://www.giustizia-amministrativa.it*.

[69] See on this point the remarks of C. Coglianese and D. Lehr, *Transparency and Algorithmic Governance*, in *Administrative Law Review,* vol. 71, no. 1, 2019.

[70] See in particular Cons. Stato, sec. VI, judgment 8 April 2019, no. 2270, in *https://www.giustizia-amministrativa.it*.

[71] See D.U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Rivista italiana di diritto pubblico comunitario*, vol. 3, 2020, 501

[72] The well-known "*General Data Protection Regulation*", EU Regulation 2016/679, *at https://gdpr.eu/tag/gdpr/.*

[73] D.U. Galetta and J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*.

to an appropriate "enhancement" of this figure that the use of ICT, from a tool in the investigation phase of the administrative procedure aimed at a mere "efficiency" of the administrative activity, can become an instrument of greater guarantee and, therefore, of general improvement of the relationship between public administration and citizens. Indeed, it is certainly not by chance that this "figure" has also attracted the attention of the European Parliament, which expressly mentions it in the context of its Resolution of 9 June 2016 on a regulation for an open, efficient and independent European Union administration.[74] Nor is it a coincidence that the NRRP has so emphatically highlighted the need to invest in the selection, training and career development's paths of civil servants.[75]

4. *Prospects opened by the National Recovery and Resilience Plan*

4.1. *Public administration reform and digital transition*

In the National Recovery and Resilience Plan (NRRP) sent by the Italian Government to the EU Commission at the end of April 2021 - and definitively approved, by means of an Implementing Decision of the Council, on 13 July (2021) - it is underlined that the "weak administrative capacity" of the Italian public sector has been an obstacle to the improvement of services offered and to public investment in recent years. And it is stated that "the NRRP addresses this rigidity and promotes an ambitious reform agenda for the public administration".[76]

The NRRP also highlights how, faced with growing numerical, demographic and training constraints[77] the Italian public administration finds itself managing a set of extremely articulated and complex rules and procedures that have been progressively stratified over time in an uncoordinated and often conflicting manner at different administrative levels (national, regional and local).[78]

In this respect, there is an interesting reference to those Country Specific Recommendations that are formulated every year by the European Council - and subsequently adopted by the Council of the European Union (obviously on a proposal from the Commission) in the form of a Recommendation addressed to the different Member States.

The Recommendation of the Council of the European Union for 2020-2021, addressed to Italy,[79] recommends to "improve (…) the effectiveness of public administration" (recommendation no. 4), stating that "An effective public administration is crucial to ensure that the measures adopted to address the emergency and support economic recovery are not slowed down in their implementation", while, as far as Italy is concerned, "Weaknesses include lengthy procedures (…), the low level of digitalisation and weak administrative capacity".[80] It also points out that "Digitalisation across public administrations was uneven prior to the crisis" and that "Online interaction between authorities and the general public was low" with a "share of administrative procedures managed by regions and municipalities that can be started and completed entirely digitally" which remains low.[81]

The NRRP therefore makes available substantial economic resources for the "digital transition",[82] with the aim of "profoundly transforming the public administration through a strategy centred on digitalisation", which is seen as "a transversal necessity".[83]

4.2. *The problem of interoperability and the necessary creation of "databases of national interest"*

The Council of the European Union's Recommendation 2020-2021 for Italy also stresses - quite significantly - how in our country the crisis "has also exposed the lack of interoperability of public digital services".[84]

[74] See European Parliament Resolution of 9 June 2016 on a regulation for an open, efficient and independent European Union administration.
[75] See. NRRP, 4, but especially 44.
[76] NRRP, 44.
[77] In this regard, the NRRP expressly refers to blocking turnover and cutting education and training expenditure for civil servants (an average of EUR 48 per employee).
[78] NRRP, 45.
[79] EU Commission, Recommendation for a Council Recommendation on Italy's 2020 National Reform Programme and delivering a Council opinion on Italy's 2020 Stability Programme, 20 May 2021, Doc. COM/2020/512 final, at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0512*.
[80] Point 24 of the Council Recommendation on Italy's 2020 National Reform Programme.
[81] Point 24 of the Council Recommendation on Italy's 2020 National Reform Programme.
[82] As much as 27% of the NRRP resources are dedicated to digital transition, as explicitly stated on 16 of the NRRP.
[83] Mission 1, Component 1of the NRRP.
[84] Point 24 of the Council Recommendation on Italy's

According to the definition provided by international dictionaries, interoperability is the "the ability of a system or component to function effectively with other systems or components".[85]

To this regard the problem is that, as a starting point, the technological infrastructure of the (Italian) public administration was the least suited to guaranteeing interoperability, since it had been developed and organised over the years in a haphazard manner, leaving decisions to the initiative of each individual administration and without an overall vision, coordination and planning.

The result was that a jungle of thousands of small autonomous data processing centres (DPCs) had been created[86]: so that, already within the Three-Year Plan for Information Technology in public administration 2017-2019[87] launched by the Agency for Digital Italy (*Agenzia per l'Italia digitale* - AGID), a specific path dedicated to digital infrastructures had been launched, as part of a more general process of digital transformation of the country.

The aim was to rationalise the system.

On the subject of interoperability, AGID had stressed that the use of the so-called "Application Cooperation"[88] between public administrations is a key element: because it is a technical solution that makes it possible to automatically exchange information between information systems and allows services[89] to be shared.

In order to identify a common solution on interoperability based on homogeneous and shared standards, AGID had already issued a couple of "technical documents" in the past few years, setting out the design and functioning of an application-cooperation-infrastructure between public administrations.

The idea is that interchange should be aimed at providing services to citizens and businesses, so as to simplify the interaction between them and the public administration.

More recently, the move is being made from the "Application Cooperation" model to a new system of interoperability in which the IT systems of the public administration must be connected to each other and, to put it simply, "speak the same language", making information available immediately where it is needed.[90]

From a technical point of view, in October 2021 AGID adopted the "Guidelines on the technical interoperability of public administrations" and the "Guidelines on technologies and standards for the security of interoperability through APIs of information systems".[91] The aim is to ensure that all public administrations comply with such guidelines, so as to guarantee the interoperability of their own systems with those of other subjects and to favour the overall implementation of the Public-Administration-Information-System (PAIS).[92]

This new interoperability model is a cornerstone of the Three-Year Plan for IT in public administration 2020-2022,[93] and is also the basis for the strategies and objectives included in the 2021-2023 update of the plan.[94]

A concrete example of interoperability is the already mentioned "National Register of Resident Population" (*supra*, par. 2.1.), which is part of the six "Databases of national interest" pursuant to art. 60, para 3-bis of the Italian Digital Administration Code, which in para 1 defines as databases of national interest "the set of information collected and managed digitally by public administrations, homogeneous in type and content and whose

2020 National Reform Programme cit.

[85] Webster's New World College Dictionary, IV Edition, 2010.

[86] This description of the "state of the art" was made a few years ago by AGID itself, the Agency for Digital Italy (see at *https://www.agid.gov.it/it*).

[87] Which can be read at *https://docs.italia.it/italia/piano-triennale-TIC/pianotriennale-TIC-doc/it/2017-2019/index.html.*

[88] "Cooperazione applicativa", which is a specific technical solution adopted in order to enhance interoperability.

[89] See par. 10 of the Three-year Plan for Information Technology in Public Administration 2017-2019.

[90] See in this regard Determination no. 406/2020 of 9 September 2020 - Adoption of the Circular containing the guideline on technical interoperability and AGID Circular no. 1 of 9 September 2020 - Guideline on technical interoperability, both at *https://trasparenza.agid.gov.it*.

[91] Determination no. 547 of 1 October 2021 Adoption of the "Guidelines on Technologies and Standards for the Security of Interoperability through APIs of Information Systems" and the "Guidelines on Technical Interoperability of Public Administrations", in *www.agid.gov.it/sites/default/files/repository_files/547_dt_dg_n_547_1_ott_2021_adozione_lg_interoperabilit_tecnica_e_sicurezza.pdf.*

[92] See at *www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/il-nuovo-modello-interoperabilita.*

[93] See at *www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pa_2020_2022.pdf.*

[94] See at *www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2021-2023.pdf.*

knowledge is relevant to the performance of the institutional functions of other public administrations (...)".

AGID specifies further that the databases of national interest are "reliable databases, homogeneous in type and content" and that they "constitute the backbone of the public information heritage" that has to be made available to all public administrations, in order to facilitate the exchange of data and avoid asking citizens or businesses for the same information several times.[95]

Unlike some of the other "Databases of national interest" mentioned in Article 60 of the Italian Digital Administration Code, the "National Register of Resident Population" already exists. While until a few years ago the personal data of citizens were scattered among almost eight thousand different municipal registers (7,903, to be precise!), as of 17 January 2022 all Italian municipalities have in fact become part of the National Register of Resident Population.[96] This will enable the Italian public administrations to communicate efficiently with each other, having a single and certain source for citizens" data; and in the near future citizens will not have to communicate their personal data or change of residence again and again to every public administration office they reach out to.[97]

It will therefore finally be possible (at least in theory) to go beyond the "self-certification model", shortening and automating all the procedures relating to personal data.[98]

In the same vein, it will be essential to work towards the complete digitalisation of health services, in particular through the "Electronic Health Record". The goal is, as the NRRP expressly states, "the creation of a homogeneous electronic health record at national level, which will become the single point of access for citizens and residents to their clinical history and to the services offered by the National Health System"[99] (*supra*, par. 2.1.).

The "Electronic Health Record" (EHR) was initially regulated by Decree 2015/178;[100] while the Ministerial Decree of 4 August 2017, amended by the Decree of 25 October 2018, regulated the national interoperability between regional health records.[101] Finally, following the changes introduced by Decree Law 34/2020 (the so-called "Decreto Rilancio"), the EHR is now activated by law and automatically fed with data.[102]

However, in order to guarantee maximum interoperability, it will be necessary to complete the creation of the "National Register of Patients" (*Anagrafe Nazionale degli Assistiti* – ANA), which is also a database of national interest pursuant to Article 60, para 3-bis of the Italian Digital Administration Code.[103] The verification of the personal data of the patient who is to receive a health service from a "regional domain" (*dominio regionale*) is in fact the necessary precondition for the proper implementation of interoperability processes.[104]

[95] *www.agid.gov.it/it/dati/basi-dati-interesse-nazionale.*

[96] On 17 January 2022, with the addition of the Sicilian municipality of San Teodoro, the process of bringing all Italian municipalities into the National Register of Resident Population was completed. See at *www.anagrafenazionale.interno.it/tutti-i-comuni-italiani-sono-in-anpr*.

[97] See at *www.anagrafenazionale.interno.it/il-progetto/i-vantaggi.*

[98] The access to the National Register of Resident Population takes place after the signing of a "User Agreement" with the Ministry and the identification and selection of the "use cases" among those provided for and corresponding to the regulatory framework applicable to the body/public administration concerned. C. Saggini, *Accesso ai dati anagrafici con Anpr: stato dell'arte, sviluppi e risvolti pratici*, at */www.agendadigitale.eu/cittadinanza-digitale/anagrafe-unica/accesso-ai-dati-anagrafici-con-anpr-stato-dellarte-sviluppi-e-risvolti-pratici.*

[99] NRRP cit., 31.

[100] Decree of the President of the Council of Ministers of 29 September 2015, no. 178, Regulation on the electronic health record.

[101] Ministerial Decree of 4 August 2017, as amended by the Decree of 25 October 2018, Amendment of the Ministerial Decree of 4 August 2017, concerning the technical modalities and telematic services made available by the national infrastructure for the interoperability of the Electronic Health Record (ESF), at *ww.gazzettaufficiale.it/eli/id/2018/11/06/18A07058/sg.*

[102] Decree Law no. 34 of 19 May 2020, Urgent measures on health, support for work and the economy, and social policies related to the epidemiological emergency from COVID-19, at *www.gazzettaufficiale.it/eli/id/2020/05/19/20G00052/s.*

[103] This database of national interest, which was established by Article 62-ter of the Italian Code of Digital Administration and is aimed at managing the administrative data of NHS patients, is owned jointly by the Ministry of Economy and Finance and the Ministry of Health. See in this regard at *https://docs.italia.it/italia/daf/pianotri-schede-bdin/it/stabile/ana.html.*

[104] In this regard, it is clearly underlined in the pages of the AGID website dedicated to the Electronic Health Record that, pending the establishment of the ANA, the national reference registry is represented by the TS System and that it is therefore required that regional and business registries correctly use the services provided by the TS/ANA System. See at

In conclusion, it must be emphasised that the interoperability of databases and systems implies a strong unitary direction at the level of the central government. Nor is it conceivable that single local administrations can alone bear the enormous costs associated with the management and technical design of the necessary technological infrastructures.

4.3. *Digitalisation of the administrative procedure and the "once-only" principle, between national and supranational level*

As regards the digitalisation of administrative procedures, the operational tool offered by AGID in this respect is the platform called "Management System of Administrative Procedures" (*Sistema di Gestione dei Procedimenti Amministrativi* - SGPA).[105]

The SGPA platform deals with document management in the context of administrative procedures, with the aim of guaranteeing proper management of documents "from production to preservation".[106]

The connection with the second aspect of the digital transition - the one that the NRRP places alongside the topic of interoperability – emerges clearly: namely, the need to introduce the principle (and objective/standard of the EU) of the "once-only", i.e. the idea that citizens and businesses have to provide their information to public administrations only once.[107]

There is no doubt that the "once-only" principle (or objective) necessarily presupposes the digitalisation of administrative procedures. In fact, the idea of the single-access-point involves two key concepts in digital-public-administration-law: the concept of electronic document[108] and the concept of document flows and IT protocol.[109]

In this regard, there are three necessary steps to be taken:

1) The registration of incoming and outgoing documents in the protocol and their assignment to the organisational units (and the issue of administrative organisation and of the necessary changes in this regard is therefore certainly a crucial one, as well[110]).

2) The dematerialisation of the processing of document flows, both incoming and outgoing (but total dematerialisation, as the "blended mode" certainly does not work).

3) The definition of the process of preservation of electronic documents, electronic files and archives as well as copies.[111]

This all involves dealing also with the very sensitive topic of the tools available to citizens to enable their identification. There is in fact a close correlation between digital identity, online services (art. 64 of the Italian Digital Administration Code) and digital procedures (art. 65 of the Italian Digital Administration Code).[112] And it is clear that a real digital transition should also imply investing in this and putting as many citizens as possible in a position to have a digital identity and to be able to benefit from the advantages it brings.

A final clarification: the "National Administrative Procedures Management System" is implemented through the definition, by AGID, of the rules for the interoperability of document flows that public administrations implement in order to join the system.[113] But what about the management of procedures at the level of "non-national" administrations? How and to what extent is it possible to guarantee the same level of digitalisation and compliance with the same standards?

The investment envisaged in this regard by the NRRP implies, first and foremost, the

www.fascicolosanitario.gov.it/it/4.1.Identificazione-Assistito.

[105] See at *www.agid.gov.it/it/piattaforme/sistema-gestione-procedimenti-amministrativi*.

[106] See document quoted in the previous note.

[107] See NRRP, 17.

[108] Article 1 of the Italian Digital Administration Code defines the electronic document as the "computerised representation of legally relevant acts, facts or data" (art. 1, letter p) as opposed to the analogue document which is the "non-computerised representation of legally relevant acts, facts or data" (art. 1, letter p-bis).

[109] See S. D'Ancona, *Il documento informatico e il protocollo informatico e il protocollo informatico*, 159.

[110] On this point see J. Burn and G. Robin, *Moving towards e-government: a case study of organizational change processes*, in *Logistics Information Management*, vol. 16, no. 1, 2003, 25; R. Gil-Garcia, *Enacting e-Government Success: An Integrative Study of Government-wide Website, Organizational Capabilities and Institutions*, Berlin, Heidelberg, 2012; N. Nurdin, R. Stockdale and H. Scheepers, *Organizational Adaptation to Sustain Information Technology: The Case of E-Government in Developing Countries*, in *Electronic Journal of e-Government*, 2012, 70.

[111] Steps 2 and 3 (and the related issues) have already been discussed in section 2, *supra*.

[112] For more details on the subject see S. D'Ancona and P. Provenzano, *Gli strumenti della Carta della cittadinanza digitale*, 234.

[113] See at *www.agid.gov.it/it/piattaforme/sistema-gestione-procedimenti-amministrativi*.

development of the "National Digital Data Platform" (*Piattaforma Digitale Nazionale Dati* – PDND, provided for by Art. 50-ter of the Italian Digital Administration Code), in order to enable (all) administrations to make their information available through digital APIs (Application Programming Interfaces).

There is also a second project that takes especially into account the supranational perspective: it is the "single digital gateway" (provided for in Regulation (EU) 2018/1724[114]) and which aims to enable harmonisation between Member States and the digitalisation of procedures and services in the EU market.

The implementation of the single digital gateway is expressly provided for within the "Digitalisation, Innovation, Competitiveness and Culture" mission of the Italian Recovery and Resilience Plan.[115]

5. *Once-only or once-again? Concluding remarks on how to "not digitalise the complication"*

In the chapter of the Italian Recovery and Resilience Plan devoted to the reforms to be undertaken (chapter 2), it is stressed out that "One of the most valuable legacies of the NRRP must be the permanent increase in the efficiency of the public administration and its decision-making capacity"; and "digitalisation of processes and services" are identified as fundamental to this perspective.[116]

However, as the previous president of our Council of State, Franco Frattini, rightly pointed out, in this process of "digital transition" we must avoid the mistake of "digitalising the complication"[117]: i.e. duplicating all the byzantine complexities of analogue/paper administration.[118]

As I have tried to explain in the previous paragraphs, the transition from traditional administration to a truly 4.0 digital administration[119] is certainly not automatic. A favourable regulatory environment and technological adaptation of administrative structures, thanks also to the resources of the NRRP, are not in themselves sufficient. What is also needed is for the rules to be applied and for the technologies to be properly used.

For this to happen, it is necessary to be fully aware of the potential of ICT and to be able to use these innovative technologies to improve the *overall* quality of public administrations.[120]

At the moment, this is certainly not the case.

One of the major problems that has emerged in recent years - and which is likely to greatly limit the potential that the digitalisation of public administrations could have in terms of achieving "good administration" - concerns the very way in which the documents held by public administrations are usually stored and which leads to fragmentation, as well as to a multiplication of "information *silos*".

The same information is repeated several times and stored in an incongruous and/or totally inconsistent way by different administrations.

The possibility of errors due to the use of outdated or even erroneous data is thus multiplied. This, moreover, corresponds to a completely opposite logic to the one already highlighted in the 2017-2019 Three-Year Plan for Information Technology in Italian public administration, which stressed that "Data must be understood as a common good, shared freely between public administrations for institutional purposes", with a view to enhancing the value of public information assets as a strategic objective for the public administration.[121]

[114] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012. *See at https://ec.europa.eu/growth/single-market/single-digital-gateway_it.*

[115] NRRP, 83.

[116] NRRP, 44.

[117] This expression was used by the President of the Italian *Consiglio di Stato* Franco Frattini in the context of the conference on "New perspectives for Administrative Law" organised at the TAR Lazio (Rome) on 24 January 2022 and chaired by him.

[118] In this regard, I refer to my remarks in D.U. Galetta, *Technological Transition in response to COVID. Scattered Thoughts on the possibility of a (Technological) transition to a Digitalized Public Administration in Italy, with the help of the Recovery and Resilience Plan*, in *CERIDAP*, vol. 4, 2021, *https://ceridaeu* (16 November 2021), 154.

[119] D.U. Galetta and J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*.

[120] See M. Bombardelli, *Informatica pubblica, E-Government e sviluppo sostenibile*, in *Rivista italiana di diritto pubblico comunitario*, vol. 5, 2002, 991.

[121] See in the 2017-2019 Three-Year Plan for Information Technology in Public Administration about the objective of "rationalising and enhancing the

In this perspective, the creation of the already mentioned "databases of national interest" provided for in Article 60 of the Italian Digital Administration Code[122] is of utmost importance.

The NRRP itself, in its introductory part (the part on "general objectives and structure of the plan"), states that it is necessary "to speed up full interoperability between public bodies and their information bases, which will make it possible to streamline public procedures thanks to the full realisation of the principle (and EC objective/standard) of 'once-only',[123] an e-government concept whereby citizens and businesses must be able to provide their information to authorities and administrations 'once only'".[124]

This need has also been clearly stated in the Italian 2020-2022 Three-Year Plan for Information Technology in public administration, one of the guiding principles of which is "once-only": i.e. public administrations must avoid asking citizens and businesses for information they have already provided.[125]

However, an objective observation of reality forces one to note that this is exactly the opposite of what currently happens when interacting with almost all Italian public administrations. Interaction with our (semi or poorly digitalised) public administrations consists in fact - essentially and mostly - in a large number of (complicated) forms to be filled in online, with blocked "fields" and thus lacking any possibility of adaptation to the specific case, should the need arise.[126] Such online forms are usually to be accompanied by plenty of documents (to be attached online, of course), most of which contain data and information that the public administrations already possess.[127] In other words, the whole thing looks much more like a "once-again interaction" than a "once-only interaction"! It is no coincidence, in fact, that in the Digital Economy and Society Index (DESI) - the index that summarises the indicators on digital performance and tracks the progress of EU countries - Italy is underperforming in the EU context also in relation to the amount of pre-filled data in the online forms available for access to services.[128]

In conclusion, it seems clear to me that there is an urgent need to address (and hopefully solve) those I have briefly mentioned here, as well as many other problematic issues that the "digital transition" in/of the public administration necessarily entails.[129] In fact, without wishing to indulge in "neo-Luddite" attitudes - which certainly cannot be shared - it seems evident to me that the only way to avoid being "swept away" by the flood of a public administration that has gone (or rather "is going") digital is for us, as administrative law scholars, to deal (albeit with difficulty) also with the essential "technicalities" related to the public administration's digital transition.[130] This is the only way in which administrative law scholars can be able to give a proper contribution in the direction of exploring not just the full potential of "public administration 4.0" in terms of greater efficiency (which is the perspective emphasised also in the Italian NRRP), but also in the perspective of acknowledging the risks that this new kind of public administration certainly entails for the citizen and the need to control such risks and

information assets of the public administration by overcoming the "silos logic"" in order to "exploit the potential of the immense wealth of data collected and managed by public administrations". (par. 4. and 4.1.), *https://docs.italia.it/italia/piano-triennale-TIC/pianotriennale-TIC-doc/it/2017-2019/index.html.*

[122] See paragraph 4.2 *above.*

[123] The origin of the "once-only" principle is in fact to be found in the EU Regulation on the single digital gateway, which aims at simplifying and improving the effectiveness of interactions with public administrations of different Member States for citizens and businesses, also avoiding duplications (total or partial) for the same information. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway for access to information, procedures and assistance and problem-solving services and amending Regulation (EU) no. 1024/2012 and, in particular, recitals 12, 40, 55, 63, 72; Art. 14 para 2.

[124] NRRP, 17.

[125] Three-year plan for information technology in public administration 2020-2022, 9.

[126] I am referring to the fact that the forms available to be filled in directly online usually do not allow any flexibility in the input of information and block the filling in of the "next field" in the event that even one of the data required in the "previous field" is missing, even though it may not be relevant in the case at hand.

[127] Copies of personal documents, identity cards, etc.

[128] See at *https://digital-strategy.ec.europa.eu/en/policies/desi*.

[129] On this point, see already G. Duni, *L'amministrazione digitale. Il diritto amministrativo nell'evoluzione telematica*, Milan, Giuffrè, 2008; D.Marongiu, *L'attività amministrativa automatizzata*, Rimini, Maggioli, 2005.

[130] In this regard, it is very useful to read, for example, the two volumes by J-C. Heudin, *Comprendre le deep learning: Une introduction aux réseaux de neurones*, Paris, Auto-Édition 2016 and J-C. Heudin, *Intelligence Artificielle. Manuel de survie*, Science-eBook, 2017.

correct mistakes.

The potential of the digital transition of public administration has in fact to be investigated with full awareness of the technical issues and of their implications; and in the perspective of exploring how much it can deliver also in terms of a better satisfaction/realisation of that right to a good administration provided for by art. 41 of the Charter of Fundamental Rights of the European Union.[131]

[131] This right - as already mentioned above, par. 3.1. – "reflects a general principle of EU law, which is applicable to Member States when they are implementing that law". So CJEU, judgment of 10 February 2022, in case Case C-219/20, *LM*, ECLI:EU:C:2022:89, point 37.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 73-82
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 06

*e-Governance and Good Administration: Examples from Estonia**

Katrin Nyman Metcalf
(Adjunct Professor of Communications Law at TalTech Law School, School of Business and Governance, Tallinn University of Technology and Senior Legal Expert at the Estonian e-Governance Academy eGA)

ABSTRACT The notion of good administration includes many different issues, both related to how the work of public officials is organised and how users of public services perceive these services. Technology supports a good administration in different ways and can help to protect rights of individuals, like better data protection, better access to services and so on. However, there are also challenges and it is important to take a total look on what e-governance means and how it should be designed. The article uses examples from Estonia, which has one of the most advanced e-governance systems in the world, to illustrate the key connecting points between e-governance and good administration. Estonia has a comprehensive interoperability system that enables the once-only principle and efficient administration. It is however essential that the increased technical possibilities to access data are not automatically translated into practical possibilities of data access, as any access needs a basis in law and must be proportional. The Estonian e-governance system uses technology to guarantee protection of rights and ensure a legal basis for data access. There are also legal tools to deal with other challenges, like access to services.

1. *Introduction*

Development of technology has affected the way public services are offered probably since carving in stone was replaced by clay tablets. The changes have been more rapid with a rapid development of technology during the past several decades, but in addition to this, what more recent technological developments have entailed is in many instances not just a possibility to do the same thing in a different way, but to actually do different things – a transformative effect of technology.[1] In the discussions about reforms of public administrations that are taking place in the 21st century, the extent and meaning of such transformation occupy a central place. It follows logically that the more transformative a technology use is, the more likely it is to raise questions that are quite unrelated to the technology as such – questions of good administration in a broad sense. In addition to having to understand whether and how people relate to the ways in which public services are offered and whether they have the physical possibility of accessing them, there may be ethical aspects linked to technology replacing the discretion of decision-makers, entirely new perceptions of administration, and so on.

The benefits of e-governance are often presented primarily as faster and more efficient administration. This already demonstrates how e-governance can benefit good administration, the definition of which tends to include many different issues, with speed and efficiency being among them.[2] At times these benefits are however set against risks for data protection or of increased divisions in society, with a need to weigh any potential benefits against risks that are presumed to be able to nullify the benefits. Is it worth sacrificing some data protection or inclusiveness in order to offer a faster and more professional service? However, such a question is based on a misconception: there is no need to make such choices if e-governance is properly planned. By having a transformative approach, technology can in fact provide many benefits for public administration, including better protection of data and easier access for all. Such benefits need to be properly integrated in the planning of e-governance, which cannot be a purely technical matter. Legal and social questions

* Article submitted to double blind peer review.

[1] "Noting that e-governance is about democratic governance and not about purely technical issues, and convinced therefore that the full potential of e-governance will be harnessed only if ICTs are introduced alongside changes in the structures, processes and ways that the work of public authorities is organised", see Council of Europe, Committee of Ministers, *Recommendation Rec(2004)15 of the Committee of Ministers to member states on electronic governance ("e-governance") and explanatory memorandum,* Strasbourg, 2004, Preamble. Available at www.coe.int.

[2] C.C. Hood and H. Z. Margetts, *The Tools of Government in the Digital Age*, London, Palgrave Macmillan, 2007, 207.

need to be integrated in the process of introducing or increasing e-governance or generally digitalising society. This should not mean that a lot of specific legislation is introduced for digital matters, but the challenge for regulators and legislators is to determine if, how and when, new and specific legal rules are needed for the new way to conduct administration. If it is just a question of doing things with new tools, existing laws will normally be sufficient as long as the key elements of digital identification and signature as well as data protection are properly addressed.[3]

This article does not deal with the aspect of use of technology to strengthen democratic processes. This is a very interesting topic that is rightly the subject of much practical and academic interest, that ranges from how technology can be physically used to support elections for example – something that became extra relevant during the Covid-19 pandemic and the restrictions on movement that this entailed –, to opportunities for more direct democracy, lobbying by a wider range of groups and of course the very question of access to trustworthy news and political information. Many of the general features mentioned in the article have a bearing also on the question of citizen participation and thus on democracy in the broad sense, but apart from this, so called e-democracy will not be specifically addressed.

In this article, examples from Estonia will be used to illustrate what e-governance means and what the potential benefits for good administration may be – while not forgetting to highlight possible risks. Estonia is one of the countries in the world with the most advanced e-governance.[4] This is based on such matters as a universal digital identity with a much used digital signature attached to it, as well as a system of interoperability of databases, which permits the seamless provision of public services from what to citizens appears as one (virtual) location. Estonia used to be known for being the first country in the world with many digital solutions – the government went paperless in 2000 and the valid form of legislation is the digital form since 2002 to mention some examples – but today, what sets Estonian e-governance apart from other countries is rather the fact that it is very comprehensive as well as used to a great extent. In this article, the Estonian examples serve as examples to illustrate the discussion rather than study-objects for a deep analysis per se. The aim of the article is to offer a perspective on what e-governance means for good administration and how to ensure the maximum positive impact with the minimum of risks.

2. *Terminology and setting the scene*

The terms e-governance and e-government are often used interchangeably, even if they do not mean exactly the same thing. E-governance is broader as it encompasses not just public governance. Neither of the terms have any authoritative, single interpretation, set out in a generally accepted convention or similar. At the same time, usually neither the slightly different understanding of the terms, nor the difference in which words that are employed, leads to practical difficulties, as the contexts will provide the necessary interpretation. Actually, it may even be beneficial that there is no very specific definition, as e-governance should be something that touches upon most areas of governance and administration, in a manner which evolves with time and place.[5]

The absence of a clear definition, however, means that different ranking tables for the status of e-governance around the world are not always very relevant, as the comparisons may include things that are not valid everywhere or that have lost their relevance with time. In some comparisons, for example,

[3] K. Nyman Metcalf, *E-governance in law and by law*, in T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*, Heidelberg, Springer, 2014, 37.

[4] Comprehensive information on what the Estonian e-governance consist of and how it works is found on https://e-estonia.com.

[5] The Council of Europe in *Recommendation Rec(2004)15* refers to Electronic Governance or e-governance without a definition, but with an understanding that the term is self-explanatory. The World Bank links the benefits of e-governance to the definition: "E-Government refers to the use by government agencies of information technologies […] that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions". See The World Bank's brief at https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government.

the ability to upload signed Pdf files was included, whereas in an advanced e-governance system (like Estonia) this was never necessary, as it was possible to sign directly online regardless of file format. One element which is often included in e-governance rankings is the access to internet. On the one hand, in countries that have e-services, this is hugely important, as without internet there will be no point to have electronic, on-line services. On the other hand, if a country has excellent internet access but does not offer online services, it does not mean that there is advanced e-governance. This is the case in many rich and developed countries (like not least the USA, which has very limited e-governance). The existence of good internet access is clearly very relevant to measure the state of digitalisation of a society broadly, but e-governance presupposes that technology is used for the benefit of governance – not just that the technical potential for doing so exists.

The position of one or other state in rankings may appear to be irrelevant other than as a PR tool for diplomats and those seeking foreign investments, but the reason for this brief discussion about such rankings and how they are made is to point to the multifaceted nature of the phenomenon of e-governance. This is pertinent if we wish to understand whether or not it is good for administration. There has been a tendency in the past few decades, increasing across various disciplines when digital technologies become more ubiquitous, to measure most things quantitatively. Indeed, the word "digital" has brought with it a tendency to reduce everything to digits. Even if it is relevant to have criteria for comparison and benchmarks for progress, something as complex as e-governance is a good example of why it is nevertheless necessary to ensure also qualitative evaluations and narratives to explain progress or problems. It is not possible to determine in a relevant manner that a certain percentage of people became so many percent less corrupt because of a specific measure, or that so many people of a certain age are happier since a service became available in a new manner. Statistics support analysis but should not replace it. The evaluation of what is "good" remains a soft value, a subjective point that may be supported by, but cannot be replaced by, quantitatively measurable criteria.

Although there is as mentioned no unified definition of e-governance, the features of interactivity and interoperability can be used to describe key elements that sets e-governance apart from just basic use of information and communication technology (ICT). Such basic uses include presenting public information on-line or providing downloadable forms. These may be important first steps, but are not enough to merit being called e-governance. Interactivity means that it is possible to complete transactions on-line; to declare or demand something or access data that is not public. To enable this, a digital identity is necessary and it is indeed not possible to go beyond a certain point in e-governance without a digital identity that is at least as secure as a traditional one. Interoperability means that databases can communicate with one-another, which makes it possible to access information from one location and which enables the once-only principle, in that once certain information exists in the system, everyone who needs this information will be able to access it and people do not have to provide the same information more than once. Interoperability is also the tool that permits transformative speed of administrative transactions.

3. *Interactivity and interoperability*

When considering interactivity and interoperability from a legal perspective and more particularly from a human rights viewpoint, several issues come to mind. Concerns for data protection[6] appear legitimate, but also questions of access to public services as this requires additional elements, not present for traditional services, namely an access to internet (and the knowledge of how to use it) and a digital identity. While it is correct that these questions should arise in the minds of those who deal with reforms to introduce or enhance e-governance, if the matters are properly addressed, there are no obstacles to the digital

[6] The best known instrument in this context is the 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 (GDPR), in force since May 2018, that has attracted global attention. It is not necessary for the purposes of this article to discuss the instrument in any detail, as so much literature exists and as it is sufficient for our purposes to note the existence of a data protection framework.

way of performing governance. One of the key suggestions to mitigate risks for data protection is the simple albeit essential advice to make sure that the question of who should have access to data is always addressed separately from the question of what access the technology enables. This will be further explained below. As for the access to services, improving access to internet on reasonable conditions and, perhaps, adding specific access possibilities for disadvantaged groups as well as development of a secure digital identity, are questions that need to be addressed together or in parallel with the establishment of interoperability and on-line services.

Let us start with a few words about digital identities and signatures. As these topics are not very new, but various examples exist worldwide, it is generally by now understood that such identities and signatures may indeed normally be more secure than traditional ones.[7] On the one hand, we all know that it is easy to copy a handwritten signature and relatively easy to pretend to be someone else of about the same age and general appearance. The way to abuse a digital identity and signature is different, with a certain mastery of technology and additional effort being necessary. On the other hand, such pretence can be made from the other side of the world, which of course vastly enlarges the potential circle of imposters. Thus, we are faced with features that per se can both better ensure identification or make it more vulnerable. In addition to this, we also need to keep in mind that the traditional legal system was well aware of the mentioned ways it was relatively easy to fake or assume identities in the traditional system, which is why we have measures such as the need to have witnesses to a signature, to be present in person with a photo ID, to do certain transactions in front of a notary or similar. In the digital system, there is a need to determine which of such means that are still relevant and, in that case, how to move them to the digital world. It should not be ignored that in some cases the result of the consideration may be that some transactions are not suitable for the digital environment – not because it would be impossible to create technological solutions, but because there are reasons to add an extra layer of security in the shape of requirements that need extra time and effort, to allow also for reflection. When Estonians present the Estonian e-governance system, it is often said in a joking manner (although it is true) that almost the only transaction you cannot do digitally in Estonia is to get married! This is not because there is some inherent feature of marriage that it would be impossible to do on-line in a country where everyone possesses a digital identity and a means to sign digitally. The reasons for requiring personal presence may of course be described as the traditional importance of the act and other "soft" reasons, but if we like, we can also explain it more pragmatically by pointing to the enforced extra time for reflection that results from having to go to a specific location and interact directly with an official. For some acts, it may be better to have to think twice, even if technology itself does not require this! This is the first of many examples that we will see in this article of non-technical considerations that need to be an integral part of creating essentially technical systems.

This article will not elaborate on different forms of digital identities or the various necessary features for their security, such as certification organisations. It is known that there are different available technological means to make secure identities and signatures and no doubt new ways will be developed. From a legal side, the area of digital identities and signatures is one in which the principle of technological neutrality of legislation has to be somewhat qualified in order to secure an important principle of a rule of law society, namely legal certainty. Theoretically, it would be possible to allow people to use various kinds of digital identities according to their preference, but as identifying oneself is such a key feature of most transactions in society, it has to be clear which identity system will be recognised in all contexts, including as evidence in court. The need to verify a signature may arise decades after it was given, in a completely different location and context. It must be possible to know that the way a transaction was performed was in accordance with law. This said, to put excessive technical detail in the law may cause problems as it would lock in the exact technical situation at a given moment in a manner that makes any

[7] Some years old, but still relevant, is M. Wang, *The Impact of Information Technology Development on the Legal Concept – A Particular Examination on the Legal concept of 'Signatures'*, in *International Journal of Law and Information Technology*, vol. 15, issue 3, 2006, 253.

technical development impossible. This can be solved by having details in regulations, decisions or other secondary legal acts, that can be amended more easily than laws, while establishing the outlines as well as the system of verification in the law.

A common obstacle to functioning e-governance is that the digital identification system is too complex and thus the uptake of it is limited. There will always be people who are enthusiastic about new technologies and make efforts to get anything new, but these people tend to be the minority in society as a whole and, furthermore, unevenly distributed among different populations groups. If the digital identity is automatically given to everyone, it is much more likely that a broader range of people will use it. In Estonia, we do not have the same difference between age groups regarding the use of electronic services. One reason is to be found in that our e-governance is already about 25 years old and thus people who were in their prime working age when many solutions came are now elderly, but it is also important that the digital identity is automatic and, as services are generally user-friendly, it is more likely that people familiarise themselves with this new way of doing things. It is not compulsory to use the digital identity, but it is automatically given to everyone and the possibility to sign is linked with the same ID-card that can be used for travelling in the EU, for identifying oneself physically, as a shop loyalty card and so on. Thus, there is no extra action needed from citizens to get the possibility to use digital identity and signature.

To achieve benefits for good administration it is essential to get away from the tendency to use new technologies to do the same thing slightly differently, instead of embracing the transformative potential of the technology. Maybe the days when people used computers only as somewhat more comfortable typewriters are quite long passed, but when it comes to data handling, we see similar tendencies. Interoperability can eliminate the need to ask someone for data and reduce the need to update databases to the minimum, but a fully interoperable system remains the exception several decades after the technology started to be used in Estonia. What an interoperable system means is that different organisations and authorities can use databases regardless of where these are located, meaning that you use the database you need for your work directly from your workstation, even if it is held by a different organisation. There is no need to ask for data to be transferred, thus eliminating risks of data leakage, as well as the risk that different people working with the same data have different versions of it. It has been mentioned above that the technical possibilities to access data and the legal possibilities to do so are different things, so the system does not provide more data access – quite the contrary. It is namely essential that questions of how the access is legally given and how it practically takes place are integrated in the design of the system. The Estonian interoperability system is called the X-road – a name given to illustrate the connection between databases, avoiding any centralisation of data. The way the need to look separately at technical possibilities and legal possibilities for data access is handled is that any data access requires that persons identify themselves. It is only when the system determines who it is who attempts to access data that this becomes accessible to the extent intended. Such intentions are set out in agreements between the organisation that possesses the database and the one that needs to (and has a basis in law to) use the data. The agreements are specific and do not give access to organisations, but to individuals – there are no "ministry computers", but regardless of device, it is through identification that access is provided. As an extra guarantee, the access leaves a "footprint", showing who accessed which data and when. Individuals can see on their pages – in the one on-line location for all public services and data[8] – which authority accessed the data, but within the authority, it is also visible who it was.[9] Thus, in essence, the need to have a purpose and proportionality for data use is built into the system.

4. *Legal obstacles?*

When working in different countries on e-governance matters, it is not unusual to hear the argument that there are legal obstacles to e-governance in general or to specific e-services. It is possible to meet this with the statement that there is no such thing as legal

[8] In this regard, see www.eesti.ee/et.

[9] A. Rull, E. Täks and A. Norta, *Towards Software-Agent Enhanced Privacy Protection*, in T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*, Heidelberg, Springer, 2014, 77.

obstacles to e-governance! This is a statement that is on purpose somewhat provocative. Evidently, like with most legal questions, the issue depends on exactly what you mean by the question or statement. Most lawyers work with application of existing laws in specific jurisdictions, to concrete circumstances at a given point in time. In such a case, there may be various legal obstacles to doing things in a new format, whether that is the digital format or some other new way of doing things. However, the process of introducing e-governance in a country or increasing the situations in which it can be used is a process of reform and should include also legal reform. It is only in recent years that it has fortunately become more common to take a comprehensive look on what e-governance means for society and thus include a wide range of persons in the teams working on related reforms. It was until recently not unusual that the process of digitalising society was led by technical specialists and thus to a large extent shaped almost exclusively by technology. This was a way in which legal obstacles could easily be created; if a technical solution was more or less completed and up-and-running, before any attention was paid to whether it was in compliance with legal requirements, what could have been dealt with through a minor adjustment to law and procedure became a serious obstacle to the validity of transactions.

Such situations are best explained by giving some examples of what kind of obstacles may arise, illustrating how this normally means quite simple and straight-forward matters, rather than legal intricacies. If a law speaks about delivering one original and so many copies, in a world of electronic data, such a requirement normally makes no sense. The law may state that certain decisions should be issued on grey paper or that an application shall be signed in blue ink – or indeed, that applications can be made during office hours. Such form requirements are common in legislation around the world and can exist in various types of laws: in procedural codes, in general administrative acts, in sector-specific legislation or in regulations, decrees and decisions issued at different levels of an administration. Some such requirements may be ignored in practice, if it is evident that they play no role in a digital administration, but there is always a risk to legal certainty if provisions exist on paper but are differently applied in practice. Thus, there is work for lawyers in relation to e-governance, but this work does not consist mainly of drafting specific laws or other rules on all matters digital, but instead of analysing existing legislation, "vacuuming" the laws for any language that does not fit with a digital world.[10] When such provisions are found, there are different options regarding what should be done. The first question to ask should however always be: what purpose is served by the requirement?

Form requirements may well have a purpose in that the format represents a specific value: we will know that a grey paper decision is different from other decisions, or we will know that from the moment someone applied for something, they need a response within so many hours, so we need to be able to determine that applications are made so that there is sufficient time for officials to deal with them. However, there are also many form requirements that exist mainly due to tradition and perhaps never fulfilled a specific, necessary role or otherwise that role has very clearly disappeared (like the need to sign with a special ink, which may have been needed to be visible on photocopies). It is only when the purpose of a requirement is understood that the next step should be taken: should such a requirement be somehow replicated in the digital world? If the answer is yes, this is an example of the need for cooperation between law and technology: technical people need to be given the task to create something that serves the same purpose in the new environment. If on the other hand it is clear that the requirements are not needed, they should be eliminated from law. This is not a technical question and needs to be addressed by people with different expertise and roles. The introduction or increase of e-governance is a good opportunity to get rid of unnecessary requirements and consequently a simplification of law becomes a useful "by-product" of the process. Legal changes as well as the need for any new, specifically "digital" laws need to be carefully considered, as there should not be too much legislation that focuses on the form of transactions.[11] For all

[10] K. Nyman Metcalf, *How to build e-governance in a digital society: the case of Estonia*, in *Revista Catalana de Dret Public*, issue 58, 2019, 1.

[11] R. H. Weber, *A Legal Lens into Internet Governance*, in L. DeNardis, D. Cogburn, N. Levinson and F. Musiani (eds.), *Researching Internet Governance* –

its advanced e-governance, Estonia does not have any specific "e-governance" or digital legislation. Instead, the focus is on the word "governance", electronic is just the means and not the end.[12]

As access to internet is needed to use electronic services, the availability of good and inexpensive access has also meant that most people have a real possibility to try electronic channels. In this context, the legal provision that there must be computers with free internet access available to the population all over the country is important. This was introduced into the Public Information Act and Public Libraries Act in 2000 and meant that Estonian public libraries were all equipped with internet-connected computers. Today the rule is less important as most people in Estonia have other ways of accessing internet; in addition to most people having some form of subscription, there are many free wi-fi spots in the country, but the psychological importance of the rule must also not be underestimated, as it indicated that the novel ideas about governance were not just of interest for a small elite in the capital. For this reason alone, such ideas could be considered in countries that come to widespread e-governance later, especially if the socio-economic conditions of the country are diverse. The public computers are still used and not infrequently for use of public services (although there is no rule that restricts them only to that purpose) by those who very infrequently need to use a service, as the people then also often ask for help from librarians.

Even if on-line services are easy to use and everyone has the necessary identity and access to internet to use them, a good e-governance system does not mean abolishing any possibility of a personal service from a human being. This does not mean that it is necessary to retain a paper-based service, but it should be possible to go to an office and deal with administrative matters, which in practice may mean that an official makes the computer entries or assists with it. This is essential not just for those who feel uncomfortable with using computers, but also for all those situations that may "fall between chairs" or for some reason not fit with the standard digital system. The fact that most transactions can be handled by people directly on-line means that the staff in different authorities will have more time to deal with direct contacts and specific requests. To add a personal note, this author has lived in several different countries and worked in even more and can attest to the fact that getting in touch with Estonian authorities is a lot less stressful than in most countries! Very limited hours for calling or waiting in phone queues is almost unheard of in Estonia.

5. *Challenges*

The various benefits of e-governance that contribute to good administration more than just by providing faster and cheaper public services have been outlined above. However, it must not be forgotten that there are also challenges. The use of more ICT in administration does not automatically and necessarily lead to a better administration. The new tools must be used in the most appropriate manner and specific risks related to technologies must not be overlooked. We are not here thinking primarily of data protection risks, which are perhaps the most commonly mentioned legal risks related to e-governance. As has been explained, technology can be used to protect data better than in a traditional paper-based world, so it is not correct to assume greater data protection risks just because the data is in digital format. Nevertheless, one of the reasons why data protection is so commonly brought up as a reason for hesitancy about using more e-governance is a good illustration of one of the challenges that needs to be addressed when transitioning to more technology use: namely, the perception of risks. Digital data like digital transactions and "documents" are intangible, which affects the image people have of them to a great extent. Protecting a document can be very physical, like locking a safe. Delivering an application on paper is also physical and we can see that the document in question has reached its destination, that it looks fine with signatures and stamps. Assets that we can touch are easier to relate to than those that only exist virtually.

The reason to focus on how people feel about new formats is not only an expression of

Methods, Frameworks, Futures, Cambridge, MA, London, MIT Press, 2020, 107.

[12] On adapting rather than making fundamental changes to legal rules, see K. K. Duvivier, *E-Legislating*, in *Oregon Law Review*, vol. 92, issue 9, 2013, 48; P. Dutt and T. Kerikmäe, *Concepts and Problems Associated with eDemocracy*, in T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*, Cham, Springer, 286.

a "soft" outlook, to be nice to people. If inhabitants of a country that introduces more and more e-governance do not trust the new way to do things, they will not use digital solutions and there will thus not be any gains of efficiency or lower costs, as the state will have to maintain other ways of accessing services or alternatively – but hardly likely in democratic societies – use resources to force people to use digital methods. The lack of popular uptake can lead to a vicious circle, when those who are tasked with designing and allocating resources to digital services see that very few people actually use them, so there is less interest in making services available, while those who may show some interest and investigate what kind of services could be accessed in the new manner will see that there is not much and consequently it is not very relevant to learn how to operate in the new environment.

One may argue that these statements are obsolete, as the on-line world is hardly new anymore. However, even before coming to the different perceptions of different groups in society, we may note that the online world still often copies the offline one to make its users understand what is what – from small things like deleting virtual documents by placing them in a virtual wastepaper basket to more significant symbolism. In fact, the tendency to replicate the "real world" look and feel of things is something that may slow down digitalisation in some contexts. This does not mean that it is necessarily a bad thing and this statement leads on to a very relevant aspect of challenges with digitalisation of administration: that of perceptions of different people. It is popular to refer to older people as being the group that is uncomfortable with online solutions, which to some extent is true in most countries but may also be a simplification. The avid social media users of today are not all young. Yes, it tends to be the case that younger people go along with new things quicker and indeed physically can handle devices faster, so older people will keep legacy digital solutions alive longer, but at the same time, the question of what different categories feel comfortable with is more complex than just related to age. It is essential to identify which groups in society that may feel less confident in the digital world and why – with such knowledge, the necessary tools can be designed to deal with this.[13]

One of the risks with introducing e-governance is that the process is led primarily by the technology. Indeed, we need to know what technology exists and it is the technology that needs to be able to address the issues that lawyers and public officials highlight, like the need for secure identification, the need to give access to only some of the data in a specific database, the need to differentiate between different people who may access the same website for different things, and so on. However, it is not the technology that should determine why and when someone needs to identify themselves or who shall have access to what data or which services, on what conditions. These are practical reasons for including different categories of people in the process of e-governance reforms. Among the necessary skills is also the ability to understand how different categories of people perceive contacts with authorities or different organisations. A service aimed at businesses, which will mainly be used by professionals can look very different from one which is aimed at those who rarely need to contact authorities. This is very obvious as a statement, but unfortunately much less obviously reflected in digital public services. Fortunately, the situation is improving in most countries and governments are learning from the private sector, where friendly-looking chatbots may help people or websites generally are inviting also for those who are not used to navigating electronically. For tech experts it will be counter-intuitive to not employ the most advanced technology, but for "ordinary people" being able to use something familiar will be valuable. Finding the balance is something that can only be done if different competences are included in the process.

To conclude the section on challenges, it is necessary to mention the specific digital challenges and risks that do exist. This is on purpose left to the last section, not because these risks may not be significant, but as discussions on challenges of e-governance or digitalisation more broadly tend to pay a lot of attention to these features and they are thus well discussed both in practice and in

[13] Inequality or even the perception of it serves to undermine trust, as discussed by E. Menéndez Sebastián and J. Ballina Diaz, *Digital citizenship: Fighting the Digital Divide*, in *European Review of Digital Administration & Law*, vol. 2, issue 1, 2021, 149.

academic literature. Data protection was mentioned above. In addition to risks related to careless handling of data, there are risks of external attacks to steal or modify data. Many of the tools described above, used in Estonia, serve to eliminate risks in the daily, regular data handling and the GDPR also primarily addresses such risks. For external, ill-intentioned attacks, other methods are needed. This does however not mean that the protection systems introduced for the regular data processing would not serve any role in the broader context. If risks due to carelessness, lack of proper competence and oversight or over-eager data collection without systems for evaluating purpose and proportionality can be eliminated, illegal and illegitimate data uses can be more easily spotted and resources can be directed to these unpredictable risks. These kinds of actions should serve as complements to technical means such as decryption.

Just like e-governance cannot be seen as something for specialists only but must become an integrated tool for the administration as a whole, cybersecurity needs to be an integrated feature of the modern state.[14] Risks are very real and very multifaceted. It is instructive to look at the National Cyber Security Index[15] created by the Estonian e-Governance Academy and note the various matters that are measured. Protection just by technical means is not possible, but in addition to education and proper legislation, technology needs to be used when possible, as the nature of the cyber world is such that the measures taken in one country cannot be sufficient to eliminate all risks. Intrusions into the "territory" of other states are easier and more likely than ever before. When promoting e-services, it is important to be open about the fact that risks do exist and to explain how these are dealt with, rather than hoping to create trust by playing down risks or speaking about them in terms that "ordinary people" do not understand. This said, such a situation is hardly an argument against e-governance as in that case, the risk of hostile action by enemies would be a reason not to build up a good state at all – as it may be attacked. The likelihood of an attack causing serious damage must be reduced and the measures to ensure this explained to citizens. Estonia involuntarily got the chance to become an example also in this field, as the country was the first country to be the victim of a concerted cyber attack from another country, already in 2007. The very digital nature of the society opened it up to be potentially badly affected but the way the systems had been designed meant that the damage was limited in time and scope. Furthermore, the event led to public attention to cybersecurity[16] and various initiatives like a cyber "home guard" for example. The cybersecurity area develops constantly and rapidly, with international standards supporting the activities of states when they address the challenges.[17]

6. *Concluding remarks*

When discussing good administration and e-governance, the range of matters to consider is wide. We have the practical tools needed to benefit from electronic services. The technical aspects of security of identification represent only one of the matters in need of consideration. People must be able to use the identification mechanism. As mentioned above, to enable interactivity and allow people to complete transactions on-line is a key step to a transformative e-governance, to something that really changes the way administration works. It is with such a system that we can actually say that the administration has become citizen-centric in that it is the individual citizen or resident that decides where and when to use public services and communicate with authorities, instead of the authorities demanding people to come at a

[14] R. Geiss and H. Lahmann, *Freedom and Security in Cyberspace: The Focus away from Military Responses toward Non-Forcible Countermeasures and Collective Threat-Prevention*, in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2013, 621. Also E. Caliskan and R. Peterson, *Technical Defence Methods, Tools, Techniques and Effects*, in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, Tallinn, NATO Cyber Defence Centre of Excellence, 61.

[15] See http://ncsi.ega.ee.

[16] It is almost difficult to believe now that before the 2007 attacks on Estonia, no country in the world had a cybersecurity strategy (at least not an officially known one) and that even for a military alliance such as NATO, before this date the only cybersecurity tools were directly related to protecting NATO´s own communications networks and not to protecting member states from the cyber viewpoint.

[17] T. Tropin, *Cybercrime. Setting international standards*, in E. Tikk and M. Kerttunen (eds.), *Routledge Handbook of International Cybersecurity*, London, New York, NY, Routledge, 2020, 151.

time and place that suits the authority. This positive effect will not arise unless most people feel comfortable with using the digital channels and are able to do so properly.

As digital identities with a possibility to sign digitally are automatically given in Estonia, the hurdle of having to get people to be sufficiently interested to take action to procure themselves with the identity disappear. There are many possible ways to securely identify oneself digitally and this is one of the (relatively few) areas where e-governance requires specific legislation, as it must be clear not only how to get the identity, but also that it is recognised fully, if need be also as evidence in court. Another positive example from Estonia is the system of interoperable databases that not only provides faster administration, but also has data protection elements built in.

The fact that there are challenges to building a secure and efficient as well as citizen-friendly e-governance should not mean that the process is not undertaken. The gains for good administration can be very important. Technology is not a threat – it is rarely good or bad in itself, but it depends on how it is used. We have shown positive examples of increasing many different elements of administration with e-governance tools. This article does not try to push other countries to adopt exactly Estonian solutions – actually, quite the opposite in the sense that what makes e-governance successful is that it is integrated into society and administration and not seen as a separate, parallel system of governance. This is achieved only when the solution is adapted to the country in question. At the same time, not everyone needs to re-invent the wheel. Estonian solutions are more than a quarter of a century old, with many upgrades along the way, and can thus present examples of the process, challenges, and solutions that others can learn from.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 83-97
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 07

*El proceso de transformación digital en Iberoamérica: las agencias digitales como autoridades regulatorias del gobierno digital**

Mirko A. Maldonado-Meléndez
(Professor at the School of Local Government of the Ibero-American Union of Municipalists Granada)

ABSTRACT The creation and implementation of regulatory organizations as authorities of the digital government in the Ibero-American countries, true governing bodies of public policies for digital transformation (and result of agreements and commitments assumed in the Ibero-American Summits of Heads of State and Government), has not been free of problems related to the legal-normative aspect, levels of autonomy or dependency, regulatory capacities or powers, organizational hierarchy, in addition to the difficulty of an exact definition. The present work addresses this problem from the current reality and points out what are the challenges that must be faced, with the consequent reforms of the institutional models of each country, so that adequate and effective governance is provided to digital development of the State.

1. *Introducción*

El presente trabajo aborda el tema de la creación e implementación de las organizaciones regulatorias del Gobierno digital en los diversos países de Iberoamérica, como entes rectores de las políticas públicas de transformación digital, que son resultado de múltiples esfuerzos, acuerdos y compromisos asumidos en las diferentes Cumbres Iberoamericanas de jefes de Estado y de Gobierno, dada la importancia de contar con órganos dedicados a la tarea de formular los planes, programas, normas, lineamientos, proyectos, conducentes a la transformación digital de sus administraciones públicas. De ello dan cuenta las denominadas cartas iberoamericanas que, a modo de soft law, han ido impregnando los ordenamientos jurídicos de tales países, decantando en las llamadas agendas digitales como verdaderas hojas de ruta en el tránsito de la administración electrónica a lo que hoy la doctrina por unanimidad ha denominado "administración digital"[1].

El funcionamiento de estas entidades y/o estructuras organizativas iberoamericanas gestoras y ejecutoras de las políticas públicas de transformación digital – ajenas a nuestra tradición jurídica romano germánica y más cercanas a la anglosajona –, no ha estado libre de problemas relacionados con la dificultad de una definición exacta, además de las posibles colisiones constitucionales (por el aspecto jurídico-normativo), niveles de autonomía o dependencia, capacidades o potestades regulatorias, jerarquía organizativa, entre otros. Por ello, el presente trabajo interpela esta problemática desde la realidad actual y señala cuáles son los retos y desafíos que deben enfrentar, de cara a algunas reformas de los modelos institucionales de cada país, de modo que se proporcione una adecuada y eficaz gobernanza al desarrollo digital del Estado[2].

---

* Article submitted to double blind peer review.
El presente trabajo, se ha desarrollado a partir de las reflexiones vertidas en un artículo reciente denominado: *La Administración pública digital en Latinoamérica: un balance sobre su implementación y el estado de la cuestión*, en A. Cerrillo i Martínez (dir.), S. Castillo Ramos-Bossini (coord.), *La Administración digital*, Madrid, Dykinson, 2022, 403.
Es propicia la oportunidad para expresar mi agradecimiento a la profa. Dra. Alejandra Boto Álvarez, por sus valiosas y acertadas opiniones surgidas con ocasión de la elaboración del presente trabajo, como de anteriores producciones académicas, cuyas sugerencias valoro y aprecio enormemente por su pertinencia y brillantez, lo que considero un gran privilegio para mí.

[1] Cfr. M. Arenilla Sáez, *La administración digital: los riesgos de la desintermediación, las escisiones y las centralizaciones*, I ed., Madrid, INAP, 2021, 350, espec. 28 y ss. Y en ese mismo sentido: C. Campos Acuña, *Administración digital e inteligencia artificial: ¿un nuevo paradigma en el derecho público?*, en C. Ramió (coord.), *Repensando la administración digital y la innovación pública*. Madrid, INAP, 2021, 109, espec. 117; también en A. Cerrillo Martínez, *Robots, asistentes virtuales y automatización de las administraciones públicas*, en *Revista Galega de Administración Pública*, n. 61, 2021, 271, espec. 281, 282.

[2] A. Barros, (14 de abril de 2019). *Gobierno Digital: Desafíos para su arquitectura institucional.* en Blog *eL ABC, escritorio de Alejandro Barros*, www.ale jandrobarros.com/gobierno-digital-desafios-para-su-arq

Los procesos de reforma y modernización de los estados latinoamericanos, acelerados con la llegada de la pandemia ocasionada por la Covid-19 - donde las medidas de distanciamiento y aislamiento social han sido una regla – fueron puestos a prueba en las capacidades instaladas de sus administraciones públicas para la prestación correcta del servicio público y la satisfacción de necesidades colectivas, en el marco de la buena administración y el fortalecimiento de una gobernanza pública digital.

Los acuerdos tomados por los jefes de Estado y de Gobierno en las cumbres iberoamericanas y la ejecución de sus compromisos, han hecho posible el avance de la administración electrónica a la transformación digital[3], en lo que la academia ha denominado la revolución 4.0, proceso que se ha ido forjando hasta devenir en la implementación de diversos entes u organismos, autoridades administrativas o agencias gubernamentales, que lideran y ejecutan las políticas de transformación digital de cada uno de los países.

Es así que la institucionalización y consolidación en el tiempo, de este tipo de estructuras gubernamentales, van a preparar e implementar una serie de propuestas técnicas y tecnológicas que apuestan, por el camino de la innovación inteligente en la gestión pública, diseñando todo un entramado institucional coordinado, interoperable y complementario en los diferentes niveles de gobierno[4].

2. *La digitalización de las administraciones públicas en Iberoamérica: sus orígenes*

Hablar del proceso de digitalización y su expansión en Iberoamérica me lleva a pensar en dos ejes principales (conectados entre sí)[5]: por un lado, el diseño de las políticas de Estado y las estrategias para la construcción de un gobierno digital y una administración digital con soporte jurídico y con estructura organizacional en el seno de los poderes públicos estatales, con base en las llamadas agendas digitales (como instrumentos orientadores de la política); y, por otro lado, la evolución paulatina del andamiaje jurídico de diseño, perfeccionamiento y aplicación de principios, derechos y garantías en favor de los administrados y ciudadanos digitales, en instrumentos normativos o pre normativos, según cada país los haya incorporado en mayor o menor grado a sus ordenamientos jurídicos, declaraciones de principios, cartas de derechos digitales, entre otros instrumentos.

A pesar de que la implementación de la administración pública digital es de reciente data y se encuentra aún en proceso de consolidación, con importantes esfuerzos regulatorios en los diversos países a nivel de políticas de estado y legislaciones nacionales, esta tendencia ha venido siendo promovida y materializada en las recomendaciones de diversos organismos internacionales: OCDE, BID, CLAD, que tienen gran influencia en los procesos de implementación de la administración digital[6].

La urgencia de hacer efectivas las medidas de distanciamiento y aislamiento social (restricciones de garantías) producto de las recomendaciones de Organización Mundial de Salud a raíz de la pandemia de la COVID-19,

uitectura-institucional.

[3] Vid. Carta iberoamericana de innovación en la gestión pública del año 2020, en especial la recomendación 42, https://clad.org/wp-content/uploads/2020/10/Carta-Iberoamericana-de-Innovacion-10-2020.pdf

[4] Apud. Carta iberoamericana de innovación en la gestión pública del año 2020.

[5] M. Maldonado-Meléndez, *La Administración pública digital en Latinoamérica: un balance sobre su implementación y el estado de la cuestión*, en A. Cerrillo i Martínez (dir.), S. Castillo Ramos-Bossini (coord.), *La Administración digital*, Madrid, Dykinson, 2022, 403, espec. 409.
Sin duda, el concepto de transformación digital, como bien apunta Pastor, "pone en relación a la tecnología con otras variables que hacen posible la innovación". A. Pastor Bermúdez, *Innovando con servicios digitales en la administración pública*, en C. Ramió (dir). *Repensando la Administración digital y la innovación pública*, , Madrid., INAP., 2021, 201. Mientras que para otros, como Valero y Cerdá, está directamente vinculado por la explotación de datos abiertos y la exigencia de gobierno abierto. J. Valero Torrijos y J.I. Cerdá Meseguer, *Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos del Covid-19*, en *Eunomia Revista en Cultura de le legalidad*, Núm. 19, 2020, 105.

[6] Cfr. Al profesor Cerrillo Martínez, cuando al referirse a La administración digital, afirmando que: "(…) es un modelo de Administración pública que contribuye a fortalecer las relaciones entre las Administraciones públicas y la ciudadanía gracias a una apertura a la ciudadanía que se basa en una mayor transparencia y en la creación de nuevos canales para la escucha de los intereses, necesidades y opiniones de la ciudadanía. de este modo, las Administraciones públicas pueden adaptar sus decisiones a las necesidades de la ciudadanía y puedan contar con su colaboración en el desarrollo de las políticas públicas y en la prestación de los servicios". A. Cerrillo Martinez, *Presentación*, en A. Cerrillo i Martínez (dir.), S. Castillo Ramos-Bossini (coord.), *La Administración digital* 25.

que fueran implantadas a nivel global como acciones necesarias para prevenir los riesgos sanitarios, no solamente evidenciaron la inmediata respuesta de los poderes públicos y del derecho administrativo latinoamericano frente a la pandemia[7], sino que además esta especie de "cuarentena" en la que se vio envuelta la administración pública en casi todos sus niveles, ha sido una especie de pistoletazo de salida para el establecimiento obligatorio (ipso facto) y en todos los niveles gobierno, de una transformación digital de la administración pública y de sus procedimientos administrativos electrónicos. La convivencia con la inteligencia artificial, robótica y algoritmos ha venido a ser inevitable y no nos resulta extraño hablar en nuestras conversaciones cotidianas, de mesas de partes virtuales y casillas electrónicas, big data, chatbots, gobernanza de datos, algoritmos de inteligencia artificial y otros mecanismos de interrelación entre la administración y el ciudadano, producto de la incorporación a la actividad administrativa de las llamadas "tecnologías disruptivas" que adquieren mayor relevancia[8].

Y tiene que ser así, porque el servicio público y la satisfacción de las necesidades colectivas no conocen de cuarentenas ni de confinamientos, al encontrarse vinculados a una serie de derechos fundamentales que en todo Estado de Derecho debe prevalecer[9]. Y porque además la administración publica constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.

Es por ello que, para explicar los orígenes de este proceso *in fieri* en Iberoamérica, es necesario remontarse a las llamadas Cartas Iberoamericanas[10] que, a la manera de guías orientadoras, han tenido como finalidad ir reconfigurando en los países miembros un nuevo marco de gobernanza pública, una administración pública innovadora, que garantice el acceso y la satisfacción de los derechos de los ciudadanos en tiempo real: que sea, por una parte, garantista, inclusiva, accesible, eficaz y eficiente en todos los niveles de las administraciones públicas y cuya transformación innovadora sea empática con el ciudadano; en concordancia con el Objetivo número 16 de la Agenda 2030, para el desarrollo sostenible.

Podríamos afirmar que estas cartas iberoamericanas vienen a ser auténticos instrumentos de carácter supranacional suscritos por los países iberoamericanos, conscientes de la necesidad de suscribir los referidos compromisos como la única manera de avanzar de manera sostenida en los objetivos de modernización de cada uno de los estados, para alcanzar el progreso. Entre las cartas, destacan:

1) Carta Iberoamericana de Gobierno electrónico, adoptada en la XVII Cumbre iberoamericana (Santiago de Chile de 2007): Garantiza el derecho fundamental de todo ciudadano de relacionarse electrónicamente con los gobiernos y administraciones públicas, a través de la reducción de la brecha digital, uso de las TIC y fortalecimiento de la sociedad de la información.
2) Carta Iberoamericana de los Derechos y Deberes del Ciudadano en Relación con la Administración Pública, adoptada en la XXXIII Cumbre iberoamericana (Panamá de 2013): Reconoce el derecho fundamental de la persona a la buena Administración Pública y de sus derechos componentes: el derecho de los ciudadanos a que los asuntos de naturaleza pública sean resueltos en el más breve tiempo, a ser

[7] M. Maldonado-Meléndez (ed.), *Presentación*, en M. Maldonado-Meléndez (Coord.), *La intervención administrativa en la prevención de riesgos sanitarios en Latinoamérica: La respuesta de los poderes públicos y del derecho administrativo latinoamericano frente a la COVID-19*., Coruña, Colex, 2021, 15.

[8] C. Benlloch Doménech y J. Sarrión Esteve, *Los Derechos fundamentales ante las aporías de la era digital*, en *Cuestiones constitucionales, Revista Mexicana de Derecho constitucional*, Núm. 46, 2022, 4. Para mayor abundamiento se puede consultar a J. Sarrión Esteve, *El Derecho constitucional en la era de la inteligencia artificial, los robots y los drones*, en A. Peréz, G. Terruel, E. Zaffiotta y M. Iadicicco (dir), S. Romboli (coord), *Setenta años de constitución Italiana y Cuarenta años de constitución Española*, Madrid, CEPC, 2020, 322.

[9] M. Presno Linera, *Derechos fundamentales e inteligencia artificial en el Estado social, democrático y digital de derecho*, en *El Cronista del Estado social y democrático de Derecho*, Núm. 100, 2022, 2-4.

[10] Fruto de la suscripción de acuerdos en las denominadas **"**Cumbres Latinoamericanas de Jefes de Estado y de Gobierno**"** de países de la región, que se celebran con relativa frecuencia y que son rigurosamente ordenadas y publicadas por el Centro Latinoamericano de Administraciones para el Desarrollo (CLAD), este Organismo público internacional, intergubernamental, cuyo propósito es la modernización de las administraciones públicas, como factor estratégico para el desarrollo económico y social.

tratados con equidad, justicia, objetividad, imparcialidad, con ocasión de los procedimientos que inicie, con una administración pública al servicio del ciudadano y de la dignidad humana.

3) Carta Iberoamericana de Gobierno Abierto, adoptada en la XXV Cumbre iberoamericana (Bogotá de 2016): Institucionaliza la transparencia y el acceso a la información, la rendición de cuentas públicas, la participación ciudadana y la colaboración para la innovación, el derecho de acceso a la información pública y los mecanismos para optimizar los estándares de integridad y gestionar de manera más eficiente y eficaz los recursos públicos, como presupuesto del Estado social y democrático de derecho.
4) Carta Iberoamericana de Innovación en la Gestión Pública, adoptada en la XXIX Cumbre iberoamericana (Andorra de 2020): Cimenta la cultura de la innovación en toda la gestión pública con la inclusión de la revolución 4.0 en todos sus procesos, transformando las políticas, los servicios, las arquitecturas institucionales, además de la capacitación y formación de los servidores y funcionarios públicos orientándolos al desarrollo de la cultura de innovación.

Es importante subrayar la creación de la Red de Gobierno Electrónico de América Latina y el Caribe[11] (Red GEALC), un espacio de encuentro y colaboración de sus países miembros, que en su momento diera a luz el denominado Marco Iberoamericano de Interoperabilidad de Gobierno Electrónico, un espacio de impulso a las "agencias iberoamericanas" de gobierno electrónico para la elaboración de sus políticas públicas, capacitación de sus funcionarios e intercambio de experiencias y soluciones en el campo del gobierno digital.

Por todo, lo que les acabo de compartir, puedo afirmar que son precisamente las Cartas Iberoamericanas han constituido el punto de partida y de consolidación, del proceso de modernización de las administraciones públicas, el proceso de transformación digital y la instrumentalización de la administración digital, con el establecimiento de las autoridades regulatorias del gobierno digital.

[11] www.redgealc.org

3. *El nacimiento de las autoridades regulatorias de gobierno digital en Iberoamérica*

A fin de concretar los acuerdos adoptados en las cumbres iberoamericanas, los poderes públicos y sus distintas administraciones dispusieron la creación de organizaciones, estructuras y/o entes rectores técnico-normativos en materia de gobierno digital cobrando disímiles nombres como: secretarías, autoridades, subsecretarías, direcciones, divisiones y/o agencias de gobierno electrónico, entre otras definiciones afines.

La creación de agencias especializadas ha sido la opción elegida para las administraciones públicas de los países de Iberoamérica, como verdaderas gestoras de las políticas públicas diseñadas por los poderes ejecutivos, dirigiendo así el proceso transformación digital de sus administraciones[12].

La función principal de estas autoridades regulatorias de lo digital consiste en elaborar y dictar normas que regulen los distintos aspectos vinculados al proceso de transformación digital, tales como: interoperabilidad de los sistemas, datos abiertos, seguridad digital, arquitectura digital que consolide una industria nacional de software, tecnologías e identidad digital, creación de políticas públicas y normas que incentiven el uso de tales tecnologías, además la formación de recursos humanos, entre otros.

Este aparente "proceso de agencificación estatal" de lo digital, a mi modo de ver, no es otra cosa que la instrumentalización del gobierno digital, que por evidentes razones trae consigo la vigencia en Iberoamérica, que toma como referente al sistema norteamericano de agencias ejecutivas estadounidenses[13], que tiene como principal característica depender directamente del poder presidencial (Ejecutivo).

Entonces, se puede afirmar que la creación de este tipo de entidades, ostenta una naturaleza jurídica que es ajena a nuestra tradición romano-germánica, por lo que bien

[12] M. Maldonado-Meléndez, *La administración pública digital en Latinoamérica: un balance sobre su implementación y el estado de la cuestión*, 420.

[13] Sobre la diferencia de agencias dependientes e independientes se puede consultar a E. Vírgala Foruria, *La Constitución y las comisiones reguladoras de los servicios de red*, Madrid, CEPC, 2004, 393, espec. 40, 44.

podría asignárseles el nombre genérico de "autoridades regulatorias" de gobierno digital, opción que engloba a las distintas administraciones públicas en Iberoamérica. Estas últimas que se han convertido en verdaderas gestoras de las políticas públicas diseñadas por los poderes ejecutivos, para dirigir el proceso transformación digital de sus administraciones[14].

En todo caso, hay que considerar también que cada país tiene sus propias particularidades constitucionales, administrativas y organizativas, las mismas que ha venido avanzando en función a sus propias realidades, lo que no ha sido obstáculo para que lo digital penetre en el tejido social y cultural. Y al Estado - no le ha quedado más opción - que asumir el liderazgo del proceso en busca de satisfacer necesidades colectivas, pero en salvaguarda del interés general, más aún en estos tiempos de los nuevos servicios ciudadano-céntricos, de modo que pueda generar confianza en los ciudadanos[15].

3.1. *Las dificultades para una definición exacta de autoridad regulatoria en lo digital*

Con el tránsito del gobierno electrónico al gobierno digital, ante el estallido de la emergencia sanitaria, se constata no solo el fenómeno de la huida del derecho administrativo sino también la huida del derecho constitucional, que consiste en la "(…) huida de los parámetros básicos que aporta el derecho constitucional a la articulación y al fundamento del poder[16]; todo ello producto de la emergencia sanitaria, que a su vez conllevó a una especie de "emergencia organizativa" en las tecno-estructuras del Estado, que han posibilitado viabilizar las recomendaciones de organismos supranacionales como OCDE, BID, concordante con los acuerdos y compromisos de la Carta iberoamericana de 2020, por la cual se recepciona dicha recomendación en los países estudiados.

No obstante que estas estructuras organizativas centralizadas poseen diferentes nombres: Agencias, Secretarias, Subsecretarias, Dirección, División, Comité, Coordinadora, con funciones específicas con base en una ley propia y en algunos casos con un estatuto y un cuerpo funcionarial y recursos financieros, dichos entes forman parte de la administración del Estado, sometidas a la ley y al derecho de cada uno de los países, lo que me ha permitido denominarles como Autoridades regulatorias de la política digital.

A ello podemos agregar, citando a la profesora BOTO, que se trata de "(…) entes con personalidad jurídica cuyo mismo denominador común (la instrumentalidad que les une con el ente matriz del que proceden) no resulta fácil de precisar (…)"; agregando que "(…) lo importante no está en los términos sino en las realidades organizativa a las que se quiere hacer referencia: entes con personalidad jurídica propia, de los que el poder público se sirve para el cumplimiento de alguno de sus fines, a cambio de reconocerles un ámbito de actuación sustancialmente autónomo"[17].

Por último, resulta interesante observar que el término "gobierno digital", es un *nomen iuris* que se encuentra ausente en la mayoría de los textos constitucionales de los países estudiados, pero que más bien, está referido a un gobierno y su administración pública organizada y jerarquizada para los fines que persigue, que incorpora tecnologías digitales, cuya operación es de forma integrada y ofrece servicios públicos en diversos canales y plataformas, en lo que hoy la doctrina conoce como gobierno digital por diseño.

3.2. *Las autoridades regulatorias de gobierno digital en Iberoamérica: su forma de organización y funciones*

Como ya lo hemos apuntado línea arriba, la instrumentalización de las políticas de transformación digital y la digitalización de las administraciones públicas en Iberoamérica, reposa en estas autoridades regulatorias de lo

[14] M. Maldonado-Meléndez, *La administración pública digital en Latinoamérica: un balance sobre su implementación y el estado de la cuestión*, 423.

[15] En ese sentido como bien lo afirma el profesor Barros "(…) el estado debe diseñar servicios pensado en la demanda y no en la oferta como lo ha venido haciendo desde hace mucho, buscando atender las necesidades de los ciudadanos (meta-trámite)". A. Barros (18 de marzo de 2022), *Transformación digital y sus dominios*, en eL Blog. *ABC escritorio de Alejandro Barros.* www.alejandrobarros.com/transformacion-digital-y-sus-dominios.

[16] A. Rallo Lombarte, *Las administraciones independientes: una aproximación constitucional*, C. Pauner Chulvi y B. Tomás Mallen (coord.), *Las Administraciones Independientes*, Valencia, Tirant lo Blanch, 2009, 337, espec. 11.

[17] A. Boto Alvarez., *La administración instrumental en el proceso*, Madrid, Reus, 2011, 496, espec. 21.

digital, bajo diversas denominaciones y características, como veremos a continuación en una mirada panorámica:

- *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento*[18] *(Uruguay).*

Se trata de una unidad ejecutora con autonomía técnica dependiente de Presidencia de la República Oriental del Uruguay. Es la responsable del gobierno electrónico e impulsar la Sociedad de la Información y del Conocimiento. Tiene la misión de liderar la estrategia de implementación del gobierno electrónico del país. Asimismo, tiene el rol de coordinación, gestión y seguimiento del grupo de trabajo encargado del armado del Plan de acción de gobierno abierto. Cuenta con una dirección y esta a su vez con un Director ejecutivo. Su sede legal, se encuentra en Montevideo.

- *Agencia de Gobierno electrónico y tecnologías de la información y comunicación - AGETIC*[19] *(Bolivia).*

Es una institución pública (entidad) descentralizada de derecho público con personalidad jurídica, autonomía administrativa, financiera, legal y técnica, con patrimonio propio, bajo supervisión del Ministerio de la Presidencia. Se encarga de desarrollar tecnología, que permita modernizar el Estado, transformar la gestión pública y reducir la burocracia. Tiene como funciones: elaborar, proponer, promover, gestionar, articular, actualizar, evaluar y hacer seguimiento del Plan de Implementación de Gobierno Electrónico, el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades públicas y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática.

Tiene una Dirección como máxima autoridad y esta a su vez, con un Director general ejecutivo designado por el Presidente de la república, mediante resolución suprema.

Su sede central se encuentra en La Paz.

- *Secretaría de Governo Digital*[20] *(Brasil).*

Es el ente estatal que lidera el Sistema de administración de los recursos de tecnología de información del Poder ejecutivo federal y es parte Secretaría especial de Desburocratización, gestión y gobierno digital (SEDGG) parte integrante del Ministerio de Economía y responsable para la definición de políticas y directrices en la transformación digital, así como del proceso de transformación de servicios públicos a lo digital, la identidad digital e integración de servicios y sistemas de gobierno y optimizar el uso de los recursos de las tecnologías de la información.

La Secretaría de Gobierno Digital, tiene entre sus funciones definir directrices, normar y coordinar proyectos de simplificación de servicios y políticas públicas de transformación digital de servicios públicos de gobernanza y compartimiento de datos y de utilización de canales digitales, así como el diseño y mejoras de arquitecturas informáticas, en el ámbito de la administración pública directa federal, autónoma y fundacional, promover acciones para la seguridad de la información y la protección de datos personales en el ámbito de la administración pública federal.

La secretaría cuenta con un Secretario, designado por portuarias (ordenanza) por el Ministro de Economía a propuesta del Presidente de la república, dada la solvente capacidad o expertise profesional (carrera funcionarial) pero tambien por afinidad política.

Su sede está en Brasilia.

- *Secretaría de Gobierno y Transformación Digital*[21] *(Perú).*

Es un organismo (de línea) que forma parte del poder ejecutivo la Presidencia del Consejo de Ministros: dirige, evalúa y supervisa el proceso de transformación digital y dirección estratégica del Gobierno Digital y ejerce la rectoría del Sistema Nacional de Transformación Digital. Esta autoridad técnico-normativo a nivel nacional en dicha materia y, el líder nacional del proceso de transformación digital, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de informática y Gobierno electrónico (digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital).

El organismo en mención cuenta con un titular: Secretaria, designada por resolución ministerial del Presidente del Consejo de

[18] www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento.

[19] www.agetic.gob.bo/ - /nosotros.

[20] www.gov.br/governodigital/pt-br/sisp/secretaria-de-governo-digital-sgd.

[21] www.gob.pe/7025.

ministros, puede emitir resoluciones de secretaria (normas administrativas) y procedimientos en dicha especialidad. Cuenta con tres órganos de apoyo: subsecretaria de política y regulación digital, la subsecretaria de tecnologías y seguridad digital y la subsecretaria de servicios e innovación digital.

Su sede se encuentra en Lima.

- *Secretaría de Innovación Pública*[22] *(Argentina).*

Entidad perteneciente a la Jefatura de Gabinete de Ministros y es la continuadora de la ex Secretaría de Gobierno de Modernización.

Este tipo de ente gubernamental esta adscrito a la Presidencia de Estado, bajo organización, se encarga de llevar las políticas públicas de digitalización de la administración pública entre ellas, el desarrollar páginas web de los ministerios, Instituciones públicas, además de los programas de alfabetización a los menos favorecidos, capacitación al cuerpo funcionarial en el uso de herramientas digitales en entornos virtuales, promoviendo la participación ciudadana. Asimismo, establecer un diseño del sistema de gestión documental digital, firma electrónica y el establecimiento del programa punto digital, que permitirá la cobertura geográfica en el territorio nacional, además de lograr la universalización del acceso a los servicios de tecnologías de la información y las comunicaciones, creando un centro nacional de datos.

Tiene una Subsecretaria que es designada por Decreto emitido por el Jefatura de Gabinete de Ministros. Responde directamente al Jefe del Gabinete. Se trata de un cargo de confianza.

Su sede está en la capital de la ciudad Autónoma de Buenos Aires.

- *Secretaría de Estado de Digitalización e Inteligencia Artificial*[23] *(España).*

Órgano administrativo, parte de la administración pública, adscrito y supervisado por el Ministerio de Asuntos Económicos y Transformación Digital, depende del Poder Ejecutivo. Está a cargo del diseño de las políticas de digitalización de la administración pública y la reforma para la mejora de la transformación digital y el desarrollo y fomento de las telecomunicaciones y la sociedad de la información.

Tiene la función de dar impulso a la digitalización del sector público, la coordinación y cooperación interministerial con otras administraciones públicas, además de otras competencias atribuidas a otros departamentos ministeriales.

Cuenta con un Director, que es nombrado por Orden ETD, por parte de la Vicepresidenta Tercera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital.

Su sede se encuentra en Madrid.

- *Secretaría de Estado para la Transição Digital*[24] *(Portugal).*

Órgano gubernamental, que depende del Ministerio de Economía y de la transición digital. Tiene como misión llevar a cabo el plan de acción para la transformación digital, cuya misión no solo sea el monitorear, sino operacionalizar e implementar las medidas previstas dicho plan y digitalizar los servicios que presta el Estado.

Cuenta con un Secretário de Estado para la Transição Digital, que es nombrado por el ministro de Economía y de la transición digital.

Su sede se encuentra Lisboa.

- *Subsecretaria de Gobierno electrónico y registro civil*[25] *(Ecuador).*

Organismo administrativo adscrito al viceministerio de tecnologías de la información y comunicación, parte integrante del Ministerio de Telecomunicaciones y de la sociedad información (MINTEL). Está encargada de gestionar y ejecutar el plan nacional de gobierno electrónico, así como la generación de políticas y normas.

Este ente tiene una subsecretaría y un Subsecretario, designados por acuerdo ministerial, para que, en representación del ente rector de gobierno electrónico, emite oficios, comunicaciones y cualquier otro documento que permita la implementación de las políticas del sector.

Su sede está en la ciudad de Quito.

- *Dirección de Gobierno Digital*[26] *(Colombia).*

Órgano de línea y asesoramiento, dependiente del Viceministro de Transformación Digital y, por ende, del Ministerio de Tecnologías de la Información y

[22] www.argentina.gob.ar/jefatura/innovacion-publica.
[23] https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/sedia.aspx.
[24] www.portugal.gov.pt/pt/gc22/area-de-governo/economia-transicao-digital.
[25] www.telecomunicaciones.gob.ec/2-2.
[26] https://gobiernodigital.mintic.gov.co/portal.

las Comunicaciones (MinTIC). La Dirección, ejerce de autoridad administrativa, para liderar la Política de Gobierno digital, es altamente técnica, encargada de formular lineamientos, estrategias y prácticas de Gobierno digital en Colombia, acompañar a servidores públicos, de nivel nacional y territorial, a mejorar su nivel de transformación digital, orientada a la generación de valor público.

Cuenta con una dirección y un Director, responsable legal designado directamente por el Ministro – MinTIC y asume el liderazgo de la política de Gobierno digital, emite las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas.

Su sede se encuentra en la capital: Bogotá.

- *División de Gobierno Digital*[27] *(Chile).*

Órgano técnico, dependiente del Ministerio de la Secretaría General de la Presidencia, cuya principal labor es definir e implementar la política pública de gobierno digital y el uso de las TIC e implementar políticas del uso de medios electrónicos entre las diversas administraciones públicas en la transformación digital de la administración chilena. Cuenta con una Jefatura representada por un Jefe de División Gobierno Digital, designado por resolución del Ministerio de la Secretaría General de la Presidencia. Emite informes técnicos, recomendaciones, propuestas técnicas, instructivos entre otros.

Su sede se encuentra en la ciudad de Santiago.

- *Coordinadora de Estrategia Digital Nacional*[28] *(México).*

Autoridad de estrategia digital nacional que, dentro de la perspectiva del derecho de organización, adquiere la forma de unidad, prestando apoyo técnico a la oficina del Presidente de la República de México. Su titular depende directamente del mandatario. Este ente, a modo de agencia, promueve, coordina y dirige la digital de la administración pública, alineada al Plan Nacional de Desarrollo, aprovechando el potencial de las TIC e integrando a la Administración Pública Federal y sus ciudadanos.

Este ente, cuenta con un coordinador de Estrategia Digital Nacional, comprometido con la innovación, apertura, transparencia y participación ciudadana de modo que pueda mejorar la inclusión digital, instrumentalizar los mecanismos de coordinación con las dependencias y entidades de la administración pública federal, para coadyuvar el cumplimiento de las políticas en materia informativa, gobierno digital.

Su sede se encuentra en ciudad de México.

- *Comité Estratégico Digital*[29] *(Paraguay).*

Es un ente gubernamental de carácter multisectorial, encargada del diseño, construcción e implementación del plan nacional de tecnologías de información en todo el sector público, de manera colaborativa y participativa con otros sectores de la sociedad, con inversión de recursos y maximización de acciones dirigidas a lograr la transformación digital del país.

Se encuentra integrado por diferentes ministros de estado, haciendo una especie de consejo estratégico de ministros, pero que a su vez cuenta con comité técnico y una secretaria general. Este órgano es el responsable del "Plan Nacional de Tecnologías de la Información y Comunicación (TIC) o también conocido como Plan Nacional de Desarrollo Paraguay (2030).

Sus miembros son designados por decreto suscrito por el presidente de la república y presidido por el Ministro del ministerio de Tecnologías de la Información y Comunicación (MITIC), quien a su vez depende del Presidente de la República (Poder ejecutivo), cuenta con dos instancias: la estratégica y la técnica y, una Secretaria general, órgano de apoyo en la gestión administrativa de la presidencia del Comité.

Su sede se encuentra en Asunción.

- *Centro Nacional de Tecnologías de la Información - CNTI*[30] *(Venezuela).*

Es una autoridad híbrida, bajo la forma de asociación civil sin fines de lucro, con personalidad jurídica y patrimonio propio, bajo tutela del Ministerio del Poder Popular para Ciencia y Tecnología, que depende íntegramente del Presidente de la República. responsable de hacer cumplir el proceso de transformación digital en Venezuela a través del Plan Nacional de Telecomunicaciones, Informática y Servicios Postales.

Cuenta con una presidencia, un consejo directivo, un director ejecutivo, designados

[27] https://digital.gob.cl.
[28] www.gob.mx/cedn.
[29] www.mitic.gov.py/noticias/comite-estrategico-digital-mitic-presento-proyectos-prioritarios-de-la-agenda-digital-ministros.
[30] www.cnti.gob.ve.

por Ministro de estado, con funciones encomendadas titular del sector, utilizando los servicios de información y la infraestructura que desarrolla el Ministerio y cualquier otra entidad de la administración pública. Emite providencias administrativas, normas técnicas y resoluciones.

Su sede está en la capital de la república: Caracas.

Vistas así las cosas, la opción de instaurar este tipo de entes, adoptada por las administraciones iberoamericanas, es de creación propia pero solo de nivel nacional, muy distinta a la visión europea comunitaria (Unión europea, que engloba a España), aunque no se puede descartar la posibilidad de contar a futuro en la región de Latinoamérica con un ente o una autoridad administrativa independiente supranacional que oriente las políticas regulatorias sobre lo digital y la inteligencia artificial (algo que la Red GEALC viene impulsando en cierta forma y con relativo éxito) y, de paso, como señala ROBLES pueda "(…) dilucidarse el problema estructural que suponen las desigualdades tecnológicas y económicas entre Estados y la necesidad de establecer mecanismos de transferencia de tecnología a los países con menos capacidades de desarrollo"[31].

3.3. *Rasgos comunes de las autoridades regulatorias del gobierno digital*

Como hemos visto anteriormente, existen en cada país de Iberoamérica distintas formas organizativas o denominaciones propias, en las que observamos, sin embargo, ciertas coincidencias, características comunes, que se encuentran presentes en las diversas autoridades regulatorias, las mismas que describimos a continuación:

- Son entes rectores en materia de gobierno y transformación de lo digital.
- Están adscritas directa o indirectamente al Poder Ejecutivo: ya sea al Ministro del sector de las telecomunicaciones, a la Secretaría de la Presidencia, a la Presidencia del Consejo de Ministros, o a la Presidencia de la República.
- Dictan normas de jerarquía infralegal, tales como directivas, oficios, circulares, informes técnicos, recomendaciones, propuestas técnicas, instructivos etc. y son responsables de su implementación y funcionamiento.
- Brindan soporte técnico a todas las entidades de las administraciones públicas.
- Supervisan el cumplimiento normativo en materia de gobierno digital en sus distintos niveles de gobierno.
- Emiten opinión técnica vinculante especializada sobre la normatividad sobre gobierno digital.
- Promueven la digitalización de los procesos y servicios de las administraciones.
- Gozan de cercanía al entorno del poder ejecutivo, lo que les permite contar con mecanismos de activación de las políticas de transformación digital.

Adicionalmente, a las características ya mencionadas, a continuación, añadimos algunos otros rasgos comunes a casi todas las autoridades regulatorias de lo digital, que a mi modo de ver podrían eventualmente constituir "desventajas" para la continuidad y unicidad de las políticas de estado, lo siguiente:

- La permanencia en el cargo de los titulares o representantes legales de las agencias o secretarias de gobierno digital, depende únicamente de la confianza y afinidad con el Ministro, Presidente del consejo de ministros y/o con el mandatario de turno.
- Al depender presupuestariamente de la Presidencia de la república, se corrobora el escaso margen de autonomía en las decisiones que involucran cuestiones políticas, no obstante que en el aspecto técnico-normativo gozan de amplia libertad para proponer al Ministro, Presidente del consejo ministros y Presidente las políticas públicas necesarias en favor de los fines institucionales para los cuales fue creado.
- A pesar que existen mecanismos de libre designación a altos cargos públicos por parte del poder ejecutivo de los países estudiados, se sugiere que estos cargos puedan ser ocupados por funcionarios con *expertise* técnico y de comprobada solvencia profesional y académica en el sector de las Tics, políticas públicas y/o relacionadas a lo digital. Solo de este modo podrá cumplir con su mandato de manera eficiente.
- Las agencias reguladoras del gobierno digital, necesitan contar con mayores competencias transversales, que le permitan coordinar acciones con las

[31] Vid. M. Robles Carrillo, *La gobernanza de las Inteligencia artificial y parámetros generales,* en *Revista electrónico de estudios internacionales* n. 39, junio 2020, 26.

diversas entidades de la administración pública, así como las potestades suficientes como para que sus dictámenes sean seguidos por aquellas.
- La transformación digital y el avance desde el gobierno electrónico al gobierno digital deben ser sostenidos en el tiempo y resistentes a los cambios políticos y es en ese sentido que la designación y nombramiento de los responsables de las agencias en lo digital, debe ser superior al periodo presidencial.
- En el desarrollo de sus políticas de transformación digital, las entidades rectoras del gobierno digital deben asegurar de modo efectivo el cierre de brechas (por exclusión y sesgos) en favor de las minorías y grupos vulnerables.

3.4. *Mecanismos de control por parte de otros poderes públicos*

Las autoridades regulatorias antes señaladas, al formar parte de la administración pública, en base a los diseños constitucionales de cada país estudiado, pueden hacer efectiva la acción de control sobre las acciones de gobierno y ser fiscalizados:
- Por los sistemas nacionales de control (acción de control interno) y además por parte de las Entidades de fiscalización superior (el control externo) [32].
- Por parte del propio Presidente de la República en función de los indicadores de gestión de los entes en su memoria institucional y, además, siguiendo la hoja de ruta en los planes de gobierno y/o promesas electorales que hizo respecto a la política digital.
- Por las Comisiones investigadoras del Congreso de la República, que se forman en el parlamento. En razón de que toda la actividad pública está sometida a control y responsabilidad, este principio es uno de los pilares sobre los que se asienta el Estado democrático de derecho[33].

Finalmente, al ser administraciones públicas y, estar sometidas a la ley y al derecho son pasibles de el Control de jueces y tribunales de la república en cuanto al test de ponderación de derechos y prevalencia del uso y disfrute de los derechos fundamentales, da un preclaro paso a ser discutida en sede judicial.

4. *La actuación de las autoridades regulatorias de transformación y gobierno digital: principales retos y desafíos*

After Hasta aquí hemos podido apreciar cómo es que las secretarías o agencias especializadas en transformación digital y gobierno electrónico, se han convertido en las principales gestoras del proceso de transformación digital en Latinoamérica, la gran mayoría de ellas con toma de decisiones centralizadas desde el Poder Ejecutivo, al cual pertenecen por adscripción al poder ejecutivo, por lo general a la Presidencia de la república, al Consejo de ministros o al Ministro del sector de las comunicaciones.

De ello podemos concluir la existencia de una ventaja importante por cercanía al poder ejecutivo, lo que permite una mayor celeridad y ejecutividad de las decisiones y el respaldo que tienen en las más altas esferas del poder, aunque eventualmente podría implicar un cierto riesgo de politización y sesgo por parte de quien designa en el cargo al jefe, secretario o director respectivo, que se acentúa por el hecho de tener un inicio de funciones de periodo similar o coincidente en el tiempo con el titular de la cartera que le hubiera designado.

Siendo que los modelos que han inspirado estas formas de organismos rectores de lo digital (a la usanza del sistema anglosajón o norteamericano), es al mando del Poder Ejecutivo o bajo su mirada, que van a diseñarse las políticas de Estado a seguir por todas las administraciones públicas en el ámbito del gobierno digital. Por tal razón, aun cuando se pretenda un cierto grado de independencia entre el Poder Ejecutivo y los reguladores, éste siempre será relativo y atenuado en tanto dichas administraciones públicas deban cumplir con una política sujeta por decisiones del Gobierno.

Ello no significa en modo alguno que estos

[32] Sobre los órganos de control en Iberoamérica, puede consultarse en M. Maldonado Meléndez, *Los Sistemas Nacionales de Control (en defensa del patrimonio público) y los tribunales de responsabilidad administrativa en Latinoamérica: hacia una visión global del sistema represivo de funcionarial de conductas irregulares*, en F. Castillo-Blanco (dir.), *Defensa del patrimonio público y represión de conductas irregulares*, Madrid, Iustel, 2020, 257-310.

[33] En ese sentido, puede verse a C. Pauner Chulvi, *La Articulación del Control Parlamentario sobre Los Espacios Libres de Control Gubernamental: Parlamento y Administraciones Independientes*, en *Revista Teoría y Realidad constitucional*, n. 19, 2007, 329-345.

entes reguladores del proceso de transformación y gobierno digital carezcan de eficacia en el ejercicio de las funciones que les han sido asignadas. Lo que sucede es que, en la práctica, se han visto enfrentadas a una realidad compleja, en esta transición de una administración presencial a un entorno digital, acelerado por la pandemia.

Lo analizado previamente, nos lleva abordar algunos aspectos que resultan relevantes con miras a considerar los retos y desafíos que enfrentan estas agencias o secretarías de gobierno digital:

4.1. *Posibles colisiones constitucionales y legales*

Dado el protagonismo que ostentan las secretarías o agencias estatales de gobierno digital en los países de Iberoamérica, no resulta difícil deducir que son una especie de "director de orquesta", en lo que concierne a la normativa sobre transformación digital, ya que son entes rectores, con potestad normativa a nivel de Poder ejecutivo.

Sin embargo, a pesar que en su condición de entes rectores en materia técnico normativa, en principio facultados a regular materias diversas, tales como: uso de datos, identidad digital, ciudadanía digital, software público, plataformas digitales, interoperabilidad, seguridad digital, portales públicos, servicios digitales, entre otros, sucede que las normas que las regulan son de categoría infra legal, pues están contenidas en directivas, circulares, oficios, lineamientos, que carecen del imperio de la ley para ser cumplidas erga omnes por todos aquellos actores involucrados en su acatamiento.

Por ello, en mi opinión, resulta prioritario que los poderes legislativos o parlamentos de los distintos estados iberoamericanos se identifiquen con los compromisos asumidos por sus Estados en las cumbres antes reseñadas, así como en su propia legislación, a fin de incluir en sus agendas legislativas, iniciativas permanentes tendientes a una mejora constante del proceso de transformación digital, perfeccionando el entramado legal e inclusive constitucional existente, en particular en lo concerniente a los derechos de los ciudadanos digitales[34].

No debe olvidarse que, a nivel de las citadas cumbres iberoamericanas, los jefes del estado y de gobierno asumieron el compromiso de implementar y modernizar sus administraciones públicas mediante la tecnología y la innovación, para lo cual es indispensable contar con regulaciones flexibles, ágiles, con un enfoque ciudadano-céntrico. Y ha sido en ese sentido que han debido adaptar sus políticas generales de gobierno hacia la creación de este entramado legal y constitucional.

A nivel de Iberoamérica, este es un desafío constante que hoy enfrentan muchos países –aunque en diferente medida –por cuanto aun carecen de un desarrollo suficiente en este ámbito en sus políticas generales de gobierno, en sus normas con rango de ley; aunado al hecho de que al momento no cuentan con verdaderas cartas de derechos digitales o de auténticos preceptos constitucionales que formulen de manera expresa estos derechos, que muchas veces se encuentran recogidos en normas reglamentarias o infra legales, por lo que al no tener un recogimiento en la Constitución, advierten un vacío que no se condice con la naturaleza y nivel de jerarquía normativa que corresponde a los derechos fundamentales de los ciudadanos.

Por ejemplo, en el caso de Perú, desde el 2018 se cuenta con una Ley de gobierno digital (Decreto Legislativo 1412). Sin embargo, en esta ley no se ha previsto un apartado, capítulo o articulado que reconozca los derechos fundamentales de los ciudadanos digitales. A tal punto que ha tenido que ser el reglamento de esta ley, publicado este año 2021 a través de Decreto Supremo del Ministerio de la Presidencia (Decreto Supremo Nun. 029 del 2021, de la Presidencia del Consejo de Ministros), el que dedique apenas un solo artículo a enunciar tales derechos.

Esto demuestra no solamente una ausencia de técnica normativa, sino que lo más grave es que estos derechos no están reconocidos ni siquiera por la ley, mucho menos por la Constitución, lo cual, en un eventual test de ponderación o de proporcionalidad, dejaría muy vulnerable al ciudadano frente al Estado.

[34] Coincido con el profesor Presno, que estos nuevos derechos o categorías jurídicas, puedan promover cambios constitucionales que, incluso, incorporen otros derechos. En M. Presno Linera, en *Revista Jurídica de Asturias*, Núm. 45, 2022, 59.

5. ***Autoridad de las agencias o secretarias de transformación digital en los organismos autónomos especiales o sectoriales y en los niveles de gobierno sub nacionales***

Las administraciones públicas de los países de Iberoamérica tienen una organización similar entre sí, cuando menos en lo que a la composición de su aparato estatal se refiere. Desde esta perspectiva, tenemos que es un rasgo común a todas las autoridades regulatorias de lo digital, que estas tienen la calidad de órganos rectores con naturaleza técnico-normativa en la materia, por encima de todos los organismos de la administración pública, máxime cuando estas autoridades se encuentran adscritas de una u otra forma al Poder ejecutivo.

En este punto, hemos creído importante incidir en la intensidad y eficacia de la autoridad que pueden tener estas agencias o secretarías de transformación digital en los denominados organismos autónomos, que pertenecen a algún sector específico (Justicia, Transporte, Comunicaciones, Producción, Economía, etc.).

En ese sentido, puede constituir un problema a considerar, el mayor o menor grado de dificultad en el proceso de alinear los planes de gobierno y transformación digital de cada organismo, con el plan y el sistema nacional liderado por las secretarías o agencias en sus respectivos países.

De una revisión de estos planes, se puede observar cómo cada uno responde a sus propios enfoques estratégicos, objetivos, políticas y normatividad especiales sectoriales, hecho que resulta lógico y razonable. En ese sentido, si bien existe una obligación formal de alineamiento de los planes sectoriales con los planes nacionales, en la práctica se observa una prevalencia de los primeros, dado que cada sector es evaluado en primer término, por el cumplimiento de sus propios objetivos y metas, lo que va dejando en segundo plano el cumplimiento del proceso de gobierno y transformación digital de escala nacional.

A ello hay que añadir la natural resistencia de los funcionarios, servidores y personal en general al interior de dichos organismos especializados sectoriales, frente a la modificación de procesos y procedimientos, la inmersión en un ecosistema digital que no siempre es bienvenido, en particular para quienes no son "nativos digitales". Y, si bien hay una generación "analógica" que ha sabido adaptarse a los cambios tecnológicos, existe otro grupo que aun presenta dificultades para "sintonizar" con la nueva cultura organizacional que debe existir en cada organismo o sector, que permita transitar hacia un gobierno digital.

Algo parecido podría ocurrir, en otra escala, a nivel de entidades de gobierno sub nacional. Es el caso de los gobiernos regionales y locales, en el caso de regímenes unitarios y descentralizados (como el caso de Perú) o de comunidades autónomas y ayuntamientos, en el caso de regímenes federales (como sucede en España); y cómo la autoridad nacional puede, eventualmente, hacer frente a la resistencia generada por las autoridades políticas o administrativas, alegando la denominada "autonomía municipal o regional".

6. ***Inteligencia artificial y robótica: la necesidad de su implementación para una rectoría normativa y técnica eficaz y eficiente***

La transformación digital de las administraciones públicas se encuentra obviamente comprometida con el desarrollo de la inteligencia artificial, para ofrecer servicios públicos de calidad, eficientes y eficaces, en el menor tiempo posible y con cierta predictibilidad, a lo que puede contribuir en mucho el uso de los algoritmos predictivos.

Es interesante, ver cada más el creciente uso de la inteligencia artificial, los asistentes virtuales, por citar el caso de "Leo" el asistente virtual da Receita Federal do Brasil o de "Eva" asistente virtual del Banco de Venezuela, el de "Diana" Dirección de impuestos y aduanas nacionales de Colombia o el de "Prometea" (Poder Judicial de la República de Argentina) que permite ayudar al justiciable y el procesamiento de datos etc., o el caso de "Julieta" (de Indecopi, en Perú), la inteligencia artificial en cuanto la orientación de trámites y consultas en la entidad, y tantos otros, cuyo uso se intensificó en gran manera a raíz de la pandemia y el confinamiento de los dos últimos años, lo cual permitió la reconexión entre las administraciones públicas y sus ciudadanos, aun cuando debemos reconocer que estos procesos no han estado exentos de dificultades y, en mucho, han excluido a quienes no son nativos digitales o no han podido adaptarse a la nueva era digital.

No obstante, es de verse que la implementación de este tipo de inteligencias artificiales está sujeto y en función del presupuesto público asignado a cada una de las administraciones, la voluntad política de quienes detentan el poder y las capacitaciones del cuerpo funcionarial, pues es sabido que los desarrolladores se encuentran en el ámbito privado y aún falta mucho para que el sector público cuente con equipos dedicados a ello, más aún por cuanto la construcción del algoritmo, el código fuente y el lenguaje de programación deben tener como fundamento las guías y lineamientos de los reglamentos y manuales de procesos de cada entidad, lo cual ralentiza su puesta en marcha.

Por ello, se hace indispensable que los gobiernos de los países de Iberoamérica adopten las decisiones políticas de buen gobierno y buena administración, para que las contrataciones e inversiones públicas sean destinadas también al desarrollo de la infraestructura necesaria, pero también de la capacitación, formación y atracción del capital humano que permita la incorporación plena de la inteligencia artificial y la robótica, para la construcción de un auténtico gobierno digital[35].

7. *La construcción de las agendas digitales y de las cartas de derechos digitales, a partir de las cartas iberoamericanas: una tarea progresiva*

No podemos dejar de mencionar en el presente trabajo a las llamadas "Agendas Digitales", que se empezaron a gestar a partir de la creación de las Secretarías de Gobierno Digital e incluso antes de éstas, por formularse en base a los diseños de las políticas públicas, dirigidos a crear las condiciones dentro de las administraciones públicas, para desarrollar un marco de gobernanza digital de la gestión pública.

Existen importantes coincidencias entre las agendas digitales de los países de Iberoamérica, al margen de los tiempos y grados de avance acordes con la realidad política, económica y social de cada país, que resulta interesante considerar.

Un rasgo común en las mencionadas agendas digitales es que todas responden a políticas públicas diseñadas por las agencias gubernamentales a cargo de su ejecución, que reposan sobre el cumplimiento de principios que son propios del derecho administrativo, como los principios de transparencia - con rendición de cuentas -, simplificación administrativa, acceso a la información pública, a la vez de conceptos comunes como participación ciudadana, gobierno inclusivo, gobierno accesible, el buen procedimiento electrónico, entre otros.

Tenemos el caso de Argentina, con su "Plan Nacional de Telecomunicaciones" y su "Programa Conectar Igualdad", que promueven la reducción de las brechas digitales y la inclusión a través de la "red federal de fibra óptica", así como la conectividad libre y gratuita con tecnología inalámbrica en espacios públicos, para lograr la alfabetización digital; modelo es adoptado por casi todos los países, con sus propios planes y programas, como es el caso de Colombia, con su plan de "ciudades inteligentes" y su concepto de "servicios ciudadanos digitales".

Existen leyes marco para el gobierno digital en algunos de los países iberoamericanos, ciertamente unos con mayor grado de desarrollo y detalle, aunque en casi todos los casos, se encuentran contenidas en normas de jerarquía inferior, tales como decretos ministeriales o directivas de inferior rango.

Sin embargo, existe una tarea aún pendiente y es que hasta la actualidad no existen verdaderas "cartas de derechos digitales" con esa denominación que hayan sido formuladas aun por ninguno de los países iberoamericanos, aunque sí algunos intentos por otorgar y reconocer la categoría de derechos fundamentales a ciertos derechos vinculados a la esfera digital[36].

Sin embargo, tenemos avances importantes, por ejemplo, en el caso de Chile, que los incluye en la llamada *protección a los neuroderechos,* como parte del texto de su nueva Constitución; pero más aun el caso de Ecuador y el de México, que ya contienen

[35] Como bien lo refiere Martín: "se trata de usar las Tics para mejorar la administración, como función y la administración, como organización pública y persona jurídica". I. Martín Delgado, *El acceso electrónico a los servicios públicos hacia un modelo de administración digital auténticamente innovador*, en T. De la Quadra Salcedo Fernández Del Castillo, J.L. Piñar Mañas (dir.), M. Barrio Andrés, J. Torregrosa V. (coord.)., *Sociedad digital y derecho,* Madrid, Ministerio de Industria, Comercio y Turismo, 2018, 181.

[36] Vide. M. Maldonado-Meléndez., *La Administración pública digital en Latinoamérica: un balance sobre su implementación y el estado de la cuestión*, 424.

disposiciones constitucionales, aunque en principio referidas a los derechos digitales, tales como el derecho a la conexión digital.

En lo que respecta al desarrollo de la infraestructura digital o a la interoperabilidad, casi todos los gobiernos han intentado desplegar esfuerzos para desarrollar estos aspectos, aunque con las limitaciones presupuestales y organizacionales de cada administración pública, como el caso de Panamá, con su plataforma centralizada denominada "Panamá en línea", o el caso de México, que ha desarrollado el llamado "Portal Ciudadano del Gobierno Federal", para acceder a cualquier instancia o ente gubernamental; el caso de Perú, con la implementación de su "Plataforma Nacional de Gobierno Digital" o el caso de Paraguay, a través del denominado "Gobierno integrado e inteligente".

Sobre el tema de ciberseguridad en el entorno digital y la protección de datos, Iberoamérica está dando importantes avances, liderados por España, qué duda cabe, teniendo en cuenta que la protección y reconocimiento de los derechos digitales deben correr en la misma vía y a la misma velocidad que los avances tecnológicos. Así, en países como Colombia, los "habilitadores transversales" de su política de gobierno digital son "la arquitectura, la seguridad, la privacidad". Ello también sucede en Perú, con la creación del "Centro Nacional de Seguridad Digital"; así como regulaciones claras en cuanto al manejo de los datos personales de los ciudadanos, para incrementar la confianza en las distintas plataformas del gobierno.

En conclusión, las agendas digitales y de las cartas de derechos digitales en Iberoamérica constituyen una manifestación del principio de Buen gobierno en la común hoja de ruta trazada, cuya centralidad se encuentra en los compromisos asumidos en las Cumbres iberoamericanas convocadas por el CLAD y plasmadas en las Cartas iberoamericanas, aun cuando tales agendas no se encuentran alineadas entre sí, ni todos los países se encuentran necesariamente en la misma página, lo que podría deberse a la falta de priorización de las políticas públicas de modernización del estado y de digitalización de las administraciones públicas, así como a la ausencia de normas de carácter obligatorio para los Estados. Por ello, ponerlas de relieve y asegurar su continuidad, más allá de quiénes ocupen el gobierno de turno, constituye uno de los principales desafíos, en especial en Iberoamérica, región marcada en los años recientes por ciclos políticos que oscilan entre periodos de calma y de inestabilidad.

8. *Reflexiones finales*

Las agencias o secretarías de gobierno digital de los países de Iberoamérica, producto de acciones concretas de Buen gobierno, se han convertido en verdaderas gestoras de las políticas públicas diseñadas por los poderes ejecutivos, para dirigir el proceso transformación digital de sus administraciones.

Existen rasgos comunes presentes en las diversas autoridades regulatorias: su calidad de entes rectores, su naturaleza de órganos técnico normativos, su dependencia del Poder ejecutivo, su rol supervisor del proceso de transformación digital de la administración pública y sus opiniones vinculantes en la materia.

La dependencia y cercanía de estas agencias o secretarías al poder ejecutivo, si bien le permite una mayor celeridad y ejecutividad de las decisiones y el respaldo al más alto nivel (Poder ejecutivo), podría implicar un cierto riesgo de politización y sesgo de parte del jefe, secretario o director designado, lo que hace peligrar su autonomía y que carezca de continuidad en el tiempo.

A pesar de su naturaleza de entes con facultad normativa, los instrumentos que emiten son de categoría infra legal, por lo que carecen del imperio de la ley para ser cumplidas erga omnes por todos aquellos actores involucrados en su acatamiento, siendo necesario perfeccionar el entramado legal y constitucional existente en los ordenamientos jurídicos de cada país, particularmente en lo relativo a los derechos de los ciudadanos digitales.

La eficacia de la autoridad de las agencias o secretarías de gobierno digital, puede verse puesta a prueba en el proceso de alinear los planes de gobierno y transformación digital de cada organismo autónomo adscrito a un sector específico, con el plan y el sistema nacional liderado por las secretarías o agencias en sus respectivos países.

Los gobiernos de los países de Iberoamérica requieren adoptar decisiones políticas de buen gobierno y buena administración, para que las contrataciones e inversiones públicas prevean el desarrollo de infraestructura (en tecnologías de información

que permita la transformación digital), así como la capacitación, formación y atracción del capital humano que permita la incorporación plena de la inteligencia artificial y la robótica, así como la utilización del software libre para la construcción de un auténtico gobierno digital.

El perfeccionamiento de las agendas digitales y la creación de verdaderas cartas de derecho digitales constituyen un reto pendiente a nivel de Iberoamérica, a partir de la hoja de ruta trazada en las Cumbres iberoamericanas convocadas por el CLAD y plasmadas en las Cartas iberoamericanas, a fin de desarrollar un auténtico marco de gobernanza digital de la gestión pública.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 99-111
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 08

*Reflections on the Need for Further Research within National Administrative Law before the EU Artificial Intelligence Act Comes into Effect: A Danish Perspective**

Hanne Marie Motzfeldt
(Professor of Administrative Law and Digitalisation, PhD, Faculty of Law, University of Copenhagen)

ABSTRACT The European Commission's proposal for a regulation on artificial intelligence may impose an unnecessary burden on public authorities in relation to overlaps with other applicable regulations when the regulation comes into effect. The Commission is aware of this as far as the GDPR is concerned and can be expected to address overlaps as part of the legislative process. However, this article points out that similar problems will arise at a national level in Denmark as Danish national administrative law is well developed in a digital context. Based on this background, and as the fundamental principles of administrative law have significant similarities within the EU Member States, further research within administrative law is encouraged in order to provide the necessary insights before the Member States' legal systems are to be adapted to the forthcoming EU regulation.

1. *Introduction*

Denmark has one of the world's most digitalised public administrations, and investments in development, and consequently, the use of artificial intelligence (hereinafter: AI) in the public sector has been growing for a long time.[1] This development gained further momentum in 2019, as the previous government published a national strategy for AI whereby, among other things, the government initiated a number of so-called signature projects. The initiation (and government funding) of an increasingly large number of signature projects has continued under the current government and has led to the relatively widespread use of AI in Danish public administration.[2]

As these projects and other AI initiatives have unfolded, it has become clear that Danish administrative law contains a number of procedural (compliance) requirements for public authorities' development and use of AI, which have similarities with – although are not identical to – a number of the proposed provisions in the EU Commission's proposal for the regulation "Laying down harmonised rules on Artificial Intelligence," the so-called "Artificial Intelligence Act" from 21 April 2021 (hereinafter: AIA). These compliance measures all revolve around a fundamental requirement of Administrative Law by Design and the fact that according to Danish administrative law, detected errors, flaws or deficiencies in any technology used by public bodies must be rectified or the use stopped if further use poses a risk of an unlawful (noncompliant) administration.[3]

Danish case law involves, among others, a requirement for prior investigation (good administration impact assessment), thorough tests and implementation measures before any technology is put into use. Public bodies are also to establish ongoing monitoring programs in order to collect information on errors, flaws or deficiencies that emerge later during the use of said technology. Furthermore, public bodies are to ensure clear allocating of tasks and responsibilities if (when) they corporate on development, use and maintenance of

* Article submitted to double-blind peer review.

[1] Https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5481, visited 17 July 2022.

[2] Ministry of Finance and Ministry of Business Affairs, *National Strategy for Artificial Intelligence*, March 2019, available at https://eng.em.dk/publications/2019/marts/national-strategy-for-artificial-intelligence, visited 17 July 2022.

[3] Compliance regulations are, according to Professor Dr Henrik Udsen, "characterised by imposing (statutory) obligations on organisations to implement various types of measures aimed at ensuring compliance with other – substantive – binding rules," H. Udsen, *Complianceret – complianceregulering som selvstændig disciplin* in C.R. Hamer, M. Andhov, E. Bertelsen and R. Caranta (eds.). *Into the Northern Light - In memory of Steen Treumer*, Copenhagen, Ex Tuto Publishing, 2022, 567.

technologies and/or the different systems interact with each other. This national regulation, which has mainly been developed via case law from the Danish Parliamentary Ombudsman, is further outlined below (section 2). After this introduction, a number of examples of the Danish use of AI are described, and how the combination of the Parliamentary Ombudsman's case law and fundamental principles of Danish administrative law regulates public authorities' development, implementation and use of AI (section 3) are illustrated. Next, the requirements of Danish administrative law are briefly compared to some of the relevant provisions and underlying accountability structures of the AIA, and it is concluded that there is a need for legal scholars to increase their research on the fundamental principles of administrative law before the AIA takes effect (section 4).

2. *The Danish Ombudsman's case law on public digitisation*

The requirement for good administration is a broad and fundamental norm in Danish administrative law which is mainly developed by the influential Danish Parliamentary Ombudsman.[4] From a historical perspective, this non-binding norm of good administration has played a significant role in the development of Danish administrative law. Historically, case law built upon the norms of good administration develops in line with societal changes, after which those parts that are not of a predominantly ethical nature, over time, take on the character of binding legal principles, which are often later codified in statutory legislation. The norm of good administration has thus functioned as a dynamic tool to ensure ongoing adjustment and development of Danish administrative law when the public sector's tasks, functioning and organisations change, and new challenges to the rule of law and legal certainty for citizens arise.[5]

The digitalisation of the Danish public administration has, during recent decades, significantly affected Danish public administration and the relationship between public bodies and citizens. Thus, it is hardly surprising that the built-in dynamics of the Danish standard of good administration have been activated in response to these changes. As a result, a relatively fine-tuned network of compliance rules has been developed, see above on the characteristics of compliance rules.

The starting point of the development of the Danish case law related to the digitalisation of the public sector was – in short – an older and technology-neutral norm that obliges Danish public authorities to establish an organisation with healthy workflows and processes as well as ensure employees are qualified for the tasks they are to perform in public service. Hence, the organisation and procedures for public authorities and the qualifications of the civil servants have to be designed to contribute to a compliant, efficient and citizen-friendly administration. As digitalisation took place, this requirement showed to include analogue as well as digital workflows, processes and organisation of public bodies and their performance of the designated tasks via technologies.[6]

> An example of the Danish Parliamentary Ombudsman's use of this core principle of good administration in relation to the use of technologies in the Danish administration is more than 20 years old and can be found in the case FOB 1992.232. The case was investigated after a citizen filed a complaint to the Ombudsman. The citizen was dissatisfied with the outcome and handling of a case concerning owed tax (and the subsequently withholding of the citizen's salary) by the former Customs and Tax Administration. Among other things, the citizen pointed out that the authorities had not responded to the citizen's letters and requests. In response, the Parliamentary Ombudsman asked whether flaws or errors in the design, structure or use of the filing system in question complicated or hindered compliance with principles of good administration (establishment of effective procedures including timely reminders).[7] The tax authorities explained that the late or missing

[4] See on the Danish Ombudsman almost monopoly-like role in developing and enforcement of Danish administrative law, H.M. Motzfeldt, *The Danish Principle of Administrative Law by Design* in *European public law*, vol. 23, No. 4, 2017, 739.

[5] N. Fenger, *Forvaltningsloven som minimumslov - 25 år efter*, in J.C Bülow, J. Møller, J. Olsen and S. Rønsholdt (eds.), *Forvaltningsloven 25 år*, Copenhagen, DJØF Publishing, 2012, 69-89. See also on the current developments related to use of technologies H.M. Motzfeldt, *Towards a legislative reform in Denmark?* in *NAVEIÑ REET: Nordic Journal of Law and Social Research*, No. 9, 2020, 117.

[6] K. Talevski, *God forvaltningsskik*, in Niels Fenger (ed.), *Forvaltningsret*, Copenhagen, DJØF Publishing, 2018, 692. This requirement is, i.a., described in FOB 1992.232, FOB 2006.165 and FOB 2008.380.

[7] FOB 1992.232.

responses were a consequence of a flaw in the digital filing system used (and ensured the Danish ombudsman that this structural problem would be handled).

So far, the more than 20-year-long development of case law related to public authorities' use of technology has resulted in sets of legal requirements that can be categorised as compliance regulations, see the characterisation by Dr Henrik Udsen in footnote 3. These requirements can be regarded as tools to ensure the effects of an unwritten principle which has crystalised itself from the obligation towards healthy workflows and processes and qualifications. With inspiration from the GDPR this principle can be termed Administrative Law by Design. According to present case law, Administrative Law by Design implies that any technology used by the public sector has to be designed and used in such a way that compliance with administrative law and the norms of good administration is supported.[8]

In the case FOB 2006.390, the Danish Parliamentary Ombudsman had become aware of a filing system used by the University of Copenhagen for administration related to public grants for students (SU). The system didn't have functionalities that allowed caseworkers to search for previous decisions based on categories or related to specific provisions in the relevant legislation. The Ombudsman raised doubts about whether the University of Copenhagen would be able to pursue a uniform practice if caseworkers were not able to search within previous cases and decisions. The office argued that support of compliance with the principle of equality presupposes that a public body's caseworkers are aware of – or at least have the opportunity to become aware of – the organisation's previous administration of a given set of rules. In the published opinion, the office of the ombudsman made it clear that filings systems are to have embedded effective search options (functionalities) if the public bodies are not to keep lists, overviews or the like of the affected types of cases.[9]

With regards to the supplementary compliance norms, *first*, the development of technologies for the Danish public administration presupposes an initial investigation of relevant regulations to be complied with. This mapping of relevant regulation is hereinafter referred to as the requirement of a good administration impact assessment. The good administration impact assessment must be initiated before a given technology is purchased (or the development begins), and a number of minimum requirements apply.

The minimum requirement for a good administration impact is a mapping of the cases and processes that will be affected by the planned technology. Further, all relevant procedural and substantive rules must be identified and described. Thereafter, the public authority has to ensure that care is exercised "in deciding how the new technology must be designed in order to comply with the mapped regulation in the various cases and processes mapped". Hereto, it may be added that the Danish Parliamentary Ombudsman considers it a prerequisite for a sound digitisation process that "the relevant legal expertise is available in all significant phases of the process, e.g., when drafting specifications and design and when carrying out tests, etc." Finally, any interaction with other systems must be uncovered and distribution of tasks and responsibilities between different units and authorities clarified.[10]

The development of case law related to the public sector's use of technology has, *secondly,* increased focus on the need for a proactive approach to the implementation of (any) new systems in public administration. Thus, public bodies are therefore to be proactive not only in regard to testing but also to ensure relevant and necessary measures to prepare the organisation before the implementation of a digital solution, e.g., educate case workers before a given technology is put into use.[11] According to Danish case law, it is to be ensured that the design and use of the technology will contribute to lawful administration in compliance with the norms of good administration before a given technology is put into use. In other words, prior and thorough testing must be carried out and

[8] H.M. Motzfeldt and A. T. Abkenar (eds.), *Digital Forvaltning – udvikling af sagsbehandlende løsninger*, Copenhagen, DJØF Publishing, 2019, 76.
[9] FOB 2006.390.

[10] The Parliamentary Ombudsman of Denmark, Generelle forvaltningsretlige krav til offentlige IT-systemer in Myndighedsguiden, overblik #13 (Requirements for public IT systems according to administrative law in Guide for Public Authorities, Guide for Public Authorities, overview # 13), available at www.ombudsmanden.dk/myndighedsguiden/specifikke_sagsomraader/generelle_forvaltningsretlige_krav_til_offentlige_it-systemer/, visited 17 July 2022.
[11] FOB 2023-7 concerning adequate testing.

precise instructions given to employees.[12]

> In the case FOB 2019-17, the Parliamentary Ombudsman investigated the Danish tax authorities' system One Tax Account (which is now remedied and still in use). In 2013, One Tax Account established an official account for every company in Denmark. Via this account, interest is to be added to the companies' tax balance daily (and this positive or negative interest is to be credited to the account monthly). The first interest was to be calculated and credited at the end of August 2013. However, this was postponed due to a deficiency in data quality and errors in the calculation algorithms. The Danish Ombudsman stated that a system with such flaws and shortcomings shouldn't have been put into operation at all
>
> The so-called health platform is a semi-automating system for the administration of different health services developed for the Capital Region and the Region of Zealand in Denmark. The platform was put in use in spite of grave malfunctions and being highly complex for users. In 2018, Rigsrevisionen (the Danish Parliamentary National Audit Office) uncovered that the two regions had implemented the platform without sufficient testing and reflection of the expected effect on the hospitals' activities and administration. Rigsrevisionen stated that the region's testing of the system and training of staff had been inadequate. In other words, Rigsrevisionen was of the opinion that the Region's preparations for the implementation of the Health Platform had been deficient and inadequate.[13]

Associated with the requirements of necessary, relevant and adequate testing and taking measures for preparing the organisation for implementation are the basic Danish principles of public leaders' responsibilities. Leaders (management) of a Danish public body are obliged to continuously monitor the administration for which they are responsible. Furthermore, if any indication of unlawful administration surfaces as a part of this monitoring (or in other ways), the management has a duty to take the relevant initiatives to restore a compliant administration.

> The Danish rules on the responsibilities (accountability) of public officials and leaders (management) are unwritten and developed via case law. An overall description can be found in an older Danish parliamentary document. Here, it is stated that leaders of public organisations are "to ensure *that* the [public body] at all times is organised in the most appropriate and economically rational manner, *that* appropriate procedures are established for the tasks carried on by the [public body], which ensures that the financial allocations are not exceeded and that the decisions taken by the [public body] are of the highest quality possible, both in relation to respect of rule of law and for the aim of the activity carried out by the [public body], *that* it employs staff with the best possible qualifications in relation to the nature of the tasks assigned to the public body in question, and *that* when needed due to the allocated resources, prioritisation of the tasks assigned to the [public body] is based on relevant considerations measured against the aim of [the public body's] activity. As part of this governing activity, [the leaders] are responsible for continuously monitoring how the administration is carried out and, where if there is an indication of non-compliance, to take the initiatives necessary for ensuring compliance, including ensuring information on an ongoing basis on the activities of the [public body]."[14]

This obligation to ensure a compliant administration also applies when technologies are used as tools to carry out the assigned tasks. Therefore, *thirdly*, focus on the need to draft and implement measures or policies that ensure ongoing monitoring of both technologies and their use, including procedures for further investigations if (or when) indications of flaws or errors are discovered, has increased recently in Danish case law.[15]

If the information provided via such procedures and policies – or otherwise – indicates that there may be errors, deficiencies or inconveniences in the design, functions or use of a digital solution that may cause decision processes or decisions that violate applicable regulations, a duty to react is triggered as in the analogue administration. Any public authority using potential flawed technology is thus obliged to investigate the situation further. If a closer examination reveals that there are in fact errors,

[12] FOB 2022-11 and FOB 2022-12.

[13] The Danish Parliament, Rigsrevisionens beretning nr. 17/2017 om Sundhedsplatformen, conveyed to The Danish Parliament with Statsrevisorernes remarks December 2018 (The National Audit Office's report no. 17/2017 on the Health Platform, conveyed to The Danish Parliament with the State Auditors' remarks December 2018), available at www.rigsrevisionen.dk/revisionssager-arkiv/2018/jun/beretning-om-sundhedsplatformen, visited 17 July 2022.

[14] The Danish Parliament, Forsvarsudvalget 2013-14, Alm.del, Bilag 60, 2014, Poul Smith Law Firm, Det retlige grundlag for vurdering af embedsmænds ansvar, (The legal framework of civil servants' responsibilities, The parliamentary Defense Committee 2013-14, General, Appendix 60, 2014), available at https://www.ft.dk/samling/20131/almdel/fou/bilag/60/1328842.pdf, visited 17 July 2022, and The Danish Supreme Court ruling referred in UfR 2009.999 H.

[15] FOB 2019-22 and FOB 2022-12.

deficiencies or inconveniences, whether the deficiencies lead to unlawful administration must be assessed. If this is the case, an additional duty to act is triggered, namely, to either stop the use of the said solution or to reprogram and so to speak fix the bug.

After the Parliamentary Ombudsman criticised the development and implementation of the Danish tax authorities' system, EFI, in the case FOB 2014-24, the tax authorities had an analysis of parts of the system performed. The analysis revealed a number of flaws and errors of varying consequences for the affected administration.[16] As a follow-up to these findings, the authorities requested an assessment of whether this led to the tax authorities being obliged to shut down the system wholly or partly. The memorandum regarding this matter – which was sent to the Danish Parliament – states that if a public body "… are aware of or have indications of that the use of a digital solution directly or indirectly leads to unlawful actions towards citizens, the public body must either refrain from using the system or ensure that any flaws are rectified manually before they have any consequences for the citizens. If, for example, fully automatic functions of a system lead to unlawful decisions directed at citizens, the public body in question must immediately rectify the flaws in the system or manually supervise and correct the affected decisions, or refrain from using the flawed parts of the system until remediation has taken place. The same applies if the system initiates non-compliant actions against citizens or, e.g., provides incorrect or misleading guidance to citizens. Conversely, if a system contains other flaws or errors of minor importance or affects the public body's use of resources or errors that can be remedied before they lead to unlawful decisions or other illegal actions against citizens, the public body may still use the system. The latter type of errors and flaws, however, entails a general risk that (manual) errors occur to a greater extent than otherwise. Such flaws must, therefore, be rectified as soon as possible."[17] In other words, depending on the nature of a flaw, error or deficiency in a given digital solution, Danish public authorities are obliged to stop the use of the said system if the flaws etc. lead to administration violating applicable regulation. If rectification of such faulty programming can be achieved via manual procedures, the system can still be used, but has to be reprogrammed to support compliance "as soon as possible".

According to Danish administrative and constitutional law the responsibility for ensuring compliance and the above measures to ensure compliance will always be on the public authority using a given technology to perform the task assigned to the authority in question. This is clearly stated in Danish case Law and also includes scenarios where there are no solutions on the market with the required design and functionalities, cf. FOB 2022-13 as one of the most recent option from the Danish Parliamentary Ombudsman.

In general, how thorough, detailed and, thereby, resource-consuming a good administration impact assessment has to be in order for a Danish public authority to act with necessary care during the development of a given technology will vary. This also applies to testing procedures, implementation measures and programs for monitoring the use of a given technology. Thus, from one area of administration to another and based on the specific circumstances, the resources needed to ensure thoroughness of investigations and measures etc. will differ. In other words, an implicit risk-based approach applies in Danish administrative law. The higher the risk of violating rule of law, fundamental principles of administrative law and the norms of good administration by using a given technology, the stricter the requirements for both, impacts assessment and the measures taken during testing, implementation and use. In particular, the risk of influencing the decisions and actions taken against citizens, and thus of violating relevant legislation, affects the need for exercising care and diligence as it

[16] Ministery of Tax, Poul Smith Law Firm, Rapport om legalitetsanalyse af EFI Delsystem funktionaliteter, Lønindeholdelse, Tvungne Betalingsordninger, og Betalingsevneberegning Budget, September 2015 (Report on legality analysis of EFI Subsystem functionalities, Wage withholding, Forced Payment Schemes, and Solvency Calculation Budget), available at https://www.skm.dk/media/6316/kammeradvokatens-legalitetsanalyse.pdf, visited 17 July 2022.

[17] The Danish Parliament, Skatteudvalget 2014-15, Alm.del, Bilag 48, Poul Smith Law Firm, Notat om SKATs anvendelse af Ét FællesInddrivelsessystem (EFI) m.v., (Responsum on SKAT's use of the One Common Recovery System (EFI) etc., Tax Committee 2014-15 General, Appendix 48), available at www.ft.dk/samling /20142/almdel/SAU/bilag/48/1549098.pdf, visited 17 July 2022.

increases in step with the risk of (systematic) errors of a substantive nature. Thus, it may be added, as previously stated, that it is of relevance whether flaws in design or functionalities can be effectively compensated via manual procedures.

To summarise, Danish administrative law sets up compliance procedures as a framework for the development and use of technologies on an accountability-like basis. Naturally, this also applies to AI-systems. At the same time, Danish administrative law – like the other European legal systems – requires that decisions taken by public authorities are based on correct information (the inquisitorial principle), respect the requirement of objectivity (legality), the principles of equality and of proportionality, etc. AI used by public authorities must, therefore, be designed to respect these fundamental principles of administrative law, see below in section 3.

3. *Requirements for AI – examples*

3.1. *Introduction*

As described above in section 1, the Danish strategy for AI provides funding for so-called signature projects. In Denmark, many such projects have thus been established annually since 2019. The projects are anchored in various public bodies, which subsequently report their experiences and challenges to the Agency of Digitalisation within the Ministry of Finance. As Danish public authorities, in general, are willing to experiment with new technologies, other AI projects have been conducted in parallel with the signature projects. As a result, a number of different tasks in the Danish public sector are supported by AI. Some examples are diagnostic technologies within the health sector and welfare tech in the care sector, such as intelligent cups able to alert elderly citizens to drink enough fluids during the day. EdTech is used as well, e.g., AI for controlling plagiarism and in learning platforms with individually adapted courses.[18]

In the following sections, however, the focus is on the development and use of AI to support or handle the processing and forming of decisions aimed at citizens. First, a number of AI technologies are described (section 3.2). Then, some of the requirements for use of such AI systems originating from the Danish administrative law are examined (section 3.3) before summarising (section 3.4).

3.2. *AI in the Danish administration and relevant administrative law principles*

In Denmark, AI is widely used to generate information (data) about conditions or circumstances that can be observed or whose accuracy can otherwise be objectively established (verifiable information). However, AI is also, to some extent, used to support or perform a variety of assessments of differing discretionary nature. With regard to the latter, there are several traditional subcategories in Danish administrative law, among others professional assessments, value estimates, expert estimates (or assessments) and legal assessments with elements of discretion.[19]

Verifiable information can, e.g., be information about geography such as the location of buildings or water sources, just as it can be information about a person's natural biological characteristics. It may also be other objective data that can be documented by observations, pictures, witnesses, weighting, etc. An example of a development project for AI generating such information for decision-making processes is the Danish Environmental Protection Agency's administration of permits for mining sand at the sea. The Agency is currently developing a system that, based on AIS data (Automatic Identification System), identifies the sailing patterns of ships mining at sea.[20] The identified patterns are to be used to determine whether a ship is mining sand and if so, estimate the amount of sand mined from the seabed. The digital formed output is, among others, to be used as a basis to monitor whether the holders of permits for sand mining comply with terms in the issued permits and for issuing invoices for the connected fees.[21] The aim is that the digital outputs will replace observations from ports'

[18] https://science.ku.dk/presse/nyhedsarkiv/2019/fristet-til-at-snyde-med-eksamensopgaven-kunstig-intelligens-opdager-dig-med-90-procent-sikkerhed/ and https://area9lyceum.com.

[19] Use of AI to detect fraud within tax and social benefit may fall into one or more of the described subcategories and raises other concerns which will not be unfolded here.

[20] AIS is a maritime radio system for the automatic identification of ships and other devices at sea. The system works by vessels equipped with an AIS radio transponder periodically transmits a digital radio message on a reserved VHF level.

[21] https://mst.dk/service/om-miljoestyrelsen/jump/raastofindvinding.

inspection staff and declarations of good faith by the holders of the permits.

Value estimates are, as the term implies, an estimate of the value of goods or income, e.g., an estimated trade price. Here, public authorities determine a matter of a factual nature by exercising an assessment of a somewhat discretionary nature involving an element of professional assessments and expert estimates. An example of the use of AI to exercise such discretionary assessment can be found within the tax administration. The Danish real estate valuation system was developed by the Danish tax authorities and is an early example of the use of machine learning. The model forms assessments (output) of the value of the real estate by being presented with a range of information about the property (input). The output is used by the tax authorities to calculate the tax on the property in question. Although some of the formed assessments have to go through manual control, and issues related to the quality of the data used to form the assessments are currently arising, the intention is that the model will generate the majority of all Danish real estate valuations in the future.[22]

Professional assessments are characterised by the need for specialised competencies, e.g., in economic, medical or environmental science. Here also, the above-mentioned Danish Environmental Protection Agency provides a Danish example. The agency has developed AI able to recognise different types of nature (habitats) from the air, i.e., categorises the various types automatically via AI based on data from satellites and, among others, drone pictures and videos.[23] The digital categorisation of the differing types of nature (output) can later be the basis for applying different terms, etc. in farming or industry permits and for reassessments, monitoring and prohibitions on the basis of the relevant laws.

From such professional assessments, there is a gradual movement towards *expert estimates*, which includes professional standards as well as a human-centred element and, to some extent, a legal assessment, as expert estimates are to be exercised in accordance with the public body's experiences, internal instructions and practices in the given area. Expert estimates frequently occur within the area of social work and a Danish example of the use of AI in this area is the robot ASTA, which was used by some municipalities until recently declared in violation of the GDPR by the Danish Data Protection Agency. ASTA could allegedly identify the citizens at risk of becoming long-term unemployed and was used as a part of case workers' guidance of unemployed citizens. ASTA was – until the Data Protection Agency's decision – under further development in order to provide suggestions for specific initiatives and decisions directed at the citizens at risk.[24]

Finally, there are *legal assessments*, when decisions or processes are based on an imprecise legal basis and, thereby, leave discretionary power to the designated public authorities. In Denmark, discretionary power is often given the executive power via indefinite wording in legislative provisions as "special circumstances", a "significant disadvantage" or a requirement for "fairness". For such legal assessments, the legal methodology requires that the sources of law are scrutinised in order to ensure that (only) the criteria legislator presumed to include in the assessments are included and to ensure that these criteria are weighed against each other in accordance with the Danish ban of misuse of powers (principles of objectivity), the principles of equality and of proportionality, etc. An illustrative Danish example of the use of AI to form legal assessments of a discretionary nature is a signature project anchored in the Municipality of Frederiksberg. The municipality is developing AI that is able to "support the employees in assessing whether an unemployed citizen's absence from an interview or job training should result in a deduction of the citizen's social benefits. The algorithm supports employees in making a decision based on training via thousands of

[22] Bill no. 211 of 3 May 2017 on the *Property Valuation Act*, general remarks, pkt. 2.13.2.4 and Expert Committee on Property Valuation and Improvement of Property Valuation, results and recommendations from the Government's external expert committee, 2014, 70.

[23] https://mst.dk/service/ommiljoestyrelsen/jump/billedgenkendelse-af-natur/ and https://mst.dk/service/nyheder/nyhedsarkiv/2022/mar/automatisk-naturgenkendelse-og-kortlaegning-af-naturomraader/, visited 17 July 2022.

[24] The Danish Data Protection Agency, *Kommuners hjemmel til AI-profileringsværktøjet Asta*, Reference number 2022-212-3676 (*Municipalities legal basis for use of the AI profiling tool Asta*), available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/maj/udtalelse-vedroerende-kommuners-hjemmel, visited 17 July 2022.

former cases and decisions, in order to support uniform assessments across the municipality."[25] If the municipality succeeds with the development project, AI will thus be used to form (a proposal for) a legal assessment of whether a citizen has a "fair reason" under the law to be absent from interviews or job training.

As can be seen from the above examples, AI is widely used in Denmark in connection with the preparation and forming of decisions directed at citizens. AI is used to assist in forming verifiable facts and value estimates and, to some extent, to exercise professional, expert and legal assessments. These subcategories are – from a Danish point of view – useful when it comes to identifying the relevant principles of national administrative law which are to be mapped via a good administration impact assessment, embedded in the design of the AI and to be upheld during use of the AI via implementation measures and subsequent monitoring of the use of the system in question. This question of identifying the relevant principles is further described and discussed in section 3.3 below.

3.3. *The legal framework*

3.3.1. *Introduction*

The aim of the principle of administrative law by design, good administration impact assessment, the requirement for thorough testing and preparation of implementation as well as measures and policies for monitoring the use of AI in the public sector, is to ensure that Danish public authorities strive for compliance with administrative law in the digital administration. The mapping of regulation needs to be taken into account when choosing the design, testing, implementing and drafting of monitoring measures and policies must therefore begin with an identification of the relevant principles and rules of administrative law. Here, one must bear in mind that according to Danish administrative law, the technology itself does not determine which principles or legislative provisions of administrative law apply. Only by examining the functions of the AI in the administrative processes is it possible to identify the relevant regulation as the underlying regulative paradigm of Danish administrative law focuses on the activities of public bodies. At the same time, reflection on the function of the AI in question will be vital for determining how extensive the measures to be taken as a part of the good administration impact assessment, tests, monitoring, etc. should be. These themes are discussed separately in the following sections 3.3.2 and 3.3.3 before summarising and concluding in section 3.3.4.

3.3.2. *Categorisations and relevant principles of administrative law*

The use of AI in the Danish public sector to form verifiable information, value estimates or professional assessments as a part of administrative processes aiming at forming decisions directed at citizens will typically be related to enquiries, that is, to state what are the relevant facts on which the decisions are to be based. The digitally formed output must, therefore, be in compliance with the Danish inquisitorial principle, see further below in this section. Value estimates, and to some extent expert estimates, differ by being regarded as relevant facts on which the decisions are to be based, but closely intertwined with the legal assessment related to the legal basis for the decision in question. The use of AI to form such estimates is therefore regulated by both the inquisitorial principle and the principles of administrative law applying to legal discretionary assessments. Finally, the use of AI for legal assessments presupposes that the AI is designed to contribute to compliance with the latter, e.g., the requirement of objectivity (legality), the principles of equality and of proportionality, etc.

Further, and elaborating on the above, the Danish inquisitorial principle is a fundamental principle of Danish administrative law which is well established in case law by both courts and the Parliamentary Ombudsman. It follows from the principle that Danish public authorities are obliged to ensure that decisions directed at citizens are based on relevant, necessary and correct information.[26] If reasonable doubt about the accuracy or quality of the information in question arises, it is the responsibility of the public authorities – not

[25] Described on Local Government Denmark's website, https://www.kl.dk/tema/kommunale-projenester-med-kunstig-intelligens/#. See also The Agency of Digitalisation, https://digst.dk/strategier/kunstig-intelligens/signaturprojenester/. Both visited 17 July 2022.

[26] Pkt. 199 in guideline no. 11740 of 4 December 1986 on the Public Administration Act.

the citizens – to carry out further investigations and ensure that the information is correct. In relation to verifiable information, such control will usually take place by verification, e.g., observations or testimonies. In the case of non-verifiable information, Danish public authorities may be obliged to obtain expertise from elsewhere, e.g., from other public authorities or from private consultants. Such expertise can be relevant to ensure that a value estimate is as close to what can be assumed to be correct as possible or that a professional assessment or expert estimate (assessment) is within the professional standards for the area in question. At the same time, public authorities must be continuously aware of any reversals by supervisory bodies or courts that may indicate a need for general changes in how such estimates or assessments are performed.[27]

The above applies regardless of whether AI is used or not. Proper use of AI in such functions thus presupposes that the AI is developed to provide the correct information in the given context. Digitally generated *verifiable information* must be aligned with reality. *Value estimates and professional assessments* have to be performed within the relevant professional standards and correspond to the practice established within the given area. The example of machine learning-based real estate value estimates described above may serve as an illustration. Looking back in time, such estimates were carried out in a purely analogous context by trained professionals who collected data about the property through various sources, supplemented by on-site inspections. During this time, the competent administrative bodies had achieved expertise and experience related to these types of estimates, i.e., an administrative practice had been established which ensured that the value judgment on a case-by-case basis was exercised on the basis of the same data and methodology.[28] Naturally, AI used to perform the same activity is to live up to similar standards.

However, when AI is used to support or take over *other expert estimates,* the exercise of assessments and discretion is somewhat free, as long as it remains within both relevant professional standards and the fundamental principles of administrative law. Therefore, public bodies have to focus on designing AI into supporting the administration in respect of both the inquisitional principle and the requirement applying for the legal assessments. Somewhat simpler are the *legal assessments* as the public authority using the AI may focus on ensuring no misuse of power by objectivity (legality), compliance with the principles of equality and of proportionality, etc.

For all of the above, public bodies are not only obliged to ensure that the design of the AI supports compliance with the inquisitional principle and the principles regulating discretionary assessments within administrative law. They will also have to perform relevant and necessary tests of the AI in question before bringing it into use. Finally, implementation and monitoring measures, policies and procedures must be established in order to ensure the detection, handling and rectification of flaws and defects. See further above in section 2.[29] What comprises the necessary and relevant investigations and measures depends on the overall assessment of the circumstances related to the AI system and its use. In other words, the proactive and reactive measures vary according to the risk of forming and issuing non-compliant decisions as it is in the very nature of the Danish administrative law to adopt a risk-based approach. This is discussed further in section 3.3.3.

3.3.3. *General risk assessment*

It is well known that biases in datasets used for developing AI, inappropriate training and testing strategies or simply a lack of attention to the preconditions of the dataset or the later use can lead to AI designed with patterns and models of criteria and weighting which may result in inaccuracies or – as relevant here - a violation of legal principles. Furthermore, if the quality of the input data during later use is not adequate, the output will be correspondingly flawed, regardless of the design of the AI. When assessing the risk of violating either the inquisitorial principle or the fundamental principles of Danish administrative law due to a given use of AI,

[27] See further FOB 2021 22.

[28] See from the tax area's value estimate also FOB 2021-22 on assessment of vehicle value, where development of the data-driven utility tool Estimatics is discussed.

[29] H.M. Motzfeldt, *Tilsyn med sagsbehandlende it-løsninger: om den digitale forvaltnings hyldevarer*, in *Nordisk Administrativt Tidsskrift*, vol. 93, no. 2, 2016, 17 ss., available at https://www.djoef-forlag.dk/sites/nat/Index.php, visited 17 July 2022.

firstly, a distinction must be made between fully automatic decision-making processes and the use of AI as decision support for a human caseworker.

With regard to *full automation*, e.g., the use of AI to select or exclude applicants for concessions, permits, funding or jobs, the digitally generated output is used without human control and verification in individual cases. Naturally, the requirements for good impact assessment, testing and implementation measures must be intensified, and significant efforts made in order to ensure that Danish public authorities do not use the AI in a way that leads to unlawful decisions towards citizens, unauthorised measures being implemented or incorrect guidance being given. Similarly, monitoring programs have to be intensive and clear procedures must be set to ensure that the use of the system is stopped if the use leads to non-compliant administration. See above in section 2.

In general, the use of AI *as decision support* can be considered less risky than full automation, as there should be constant human control. Still, according to Danish administrative law, flawed AI as a support tool for human caseworkers will be regarded as "errors that can be remedied before they lead to unlawful decisions or other illegal actions against citizens". Such flaws or errors "entail a general risk that (manual) errors occur to a greater extent than otherwise".[30] Naturally, public authorities are to ensure a sound combination of digital and analogue workflows effectively preventing errors and shortcomings before the AI is put into use, and effective procedures afterwards in order to detect overlooked flaws or deficiencies that occur later (and rectify therein).

A key factor in assessing how extensive the proactive and reactive measures that must be taken in relation to the development and use of AI as decision support should be is the risk of violating national administrative law, see above in section 3.3.2. In connection herewith and as a supplementary, a factor of considerable weight might be whether affected citizens have true access to challenge the digital outputs and the use of these via (especially) courts.

For the use of AI to generate *verifiable information*, it is characteristic that such outputs can be proven (or disproved) via mere documentation. In the example given in section 3.2, the Danish Environmental Protection Agency can, e.g., monitor the AI performance by comparing digitally generated outputs with random checks carried out by the port authorities. From a citizen's point of view, e.g., permit holders are able to (relatively easily) document the amount of sand collected and thereby challenge the generated output.

For *value estimates*, if necessary resources are set aside, the public body using the AI forming such estimates can monitor compliance with the inquisitorial principle based on, e.g., random comparisons with experts' professional estimates.[31] From a citizen-oriented perspective, on the other hand, it will be somewhat more difficult for a citizen to challenge a digitally formed value estimate than it is to challenge verifiable information. This is not only because public authorities are typically granted a certain margin by courts in such matters, and the citizens, therefore, normally have to prove significant deviations. Difficulties also arise due to the fact that the citizen will, normally, have to present corrective professional assessments, which makes legal proceedings more resource-intensive financially.

With regard to *professional assessments*, according to the Danish inquisitorial principle, such assessments are to respect professional standards in the area in question, see above in section 3.3.2. In the example of categorising types of nature by AI described in section 3.3.3, this will be the professional standard of biologists and closely related environmental professionals. The digitally generated outputs thus supplement (take over) the work that employed biologists and similar professionals undertook in the analogue administration. In other words, video and pictures (input data) combined with AI replace former human observations and interpretation thereof. Even though Danish administrative law obliges public bodies to ensure qualified employees exercise such assessments this can hardly apply directly to AI. On the other hand, the norms of good administration dictate that digital outputs should be of the same quality

[30] The Danish Parliament, Notat om SKATs anvendelse af Ét Fælles Inddrivelsessystem (EFI) m.v., 8. September 2015.

[31] H. Gammeltoft-Hansen, *Ombudsmandens prøvelses-begrænsninger*, in P. Blume, K. Ketscher og S. Rønsholdt (eds.), *Liv, arbejde og forvaltning*, Copenhagen, GadJura, 1995, 175.

and live up to the professional standards, as the AI otherwise poses a risk to the administration in question. Thus, if there are indications that the AI does not categorise the types of nature correctly according to professional standards, the inquisitorial principle obliges effective control before the output is used as a basis for applying regulation and forming decisions directed at citizens. Such control may be carried out via supplementary professional assessments either from the authority's employees, from other authorities or from private consultants (with the necessary professionalism). As for value estimates, it is thus realistic – if resources are set aside for this – to monitor the assessments formed. Such monitoring can, e.g., be based on random comparisons with experts' professional assessments. Information on the outcome of court proceedings may also be used for measuring whether the AI forms qualified assessments (output). From a citizen-oriented angle, however, it will at least be as resource-intensive to challenge such professional assessments as for the value estimates, as the citizen in question often will have to obtain one or more alternative professional opinions.

The complexity, and thereby the risk, seem to increase when AI is used to support the *expert estimates (assessments)*. The use of AI to form expert assessments is characterised by having both the risk elements seen in the digital exercise of the professional assessments and elements that characterise the legal assessments. This can be seen in the example of ASTA described in section 3.3.1. ASTA formed assessments, which a specialised social worker would otherwise perform using a combination of an individual impression of the specific citizen, the caseworker's experience and professionalism as well as the public authority's practice within the area. Random checks may be established via verification by human caseworkers, i.e., the output can be compared with assessments from human social workers, but court proceedings might not be very useful as expert estimates are rarely intensively reviewed by the courts. Thus, from a citizen's point of view, the outputs of ASTA will be worryingly difficult to challenge as the margin of discretion is wide and supplementary independent expert assessment within this margin will rarely lead to adjustments of the decision based on the output (expert assessment generated by the AI).

Public authorities may be able to supervise and monitor the legality (compliance) of digitally formed *legal assessment,* and in general, from a public sector point of view, this will be less complicated than the scenarios described above, as public authorities are given a very wide margin by the Danish courts in this respect. Monitoring must, therefore, as a starting point, focus on whether the principles of legality (objectivity), equality, proportionality, etc. are supported by the design of the AI and the procedures for the use thereof. Here, however, some variants of AI might be more problematic than others, as difficulties increase if the accountable public authority is unable to control the criteria embedded and the weighting thereof. From a citizen's point of view, a digital output based on discretionary powers is extremely difficult to challenge in courts as citizens will, among other things, need access to information on which criteria are used and the weight these criteria are given. Here, according to the Danish Public Administration Act, the obligation for public authorities to give reasons for their decisions directed at citizens includes an obligation to state which criteria have been decisive. This will apply to decisions formed via the use of AI as well, and thus citizens' difficulties for legal certainty of citizens' does not immediately appear to be either strengthened or weakened due to the use of AI for legal assessments. However, due to the difficulties in ensuring judicial control via courts, flaws, errors or inadequacies might affect a larger number of decisions before the effect hereof is detected and remedied, and this is naturally worrying in terms of legal certainty.

In summary, if risk and efforts in measures to ensure compliance are to follow each other, significant efforts must be made when AI is developed and used for full automation. However, this does not mean that the use of AI as decision support is risk-free, as such AI according to the Danish norms of good administration also are to support legal and sound administration. How extensive the measures that need to be taken depends on a number of factors. Since verifiable outputs are relatively easy to challenge, the use of AI to generate such data seems to be less worrying than the other uses. From here, legal certainty concerns seem to increase, especially for the citizens concerned, as it becomes more

difficult to control, verify and possibly detect whether outputs are generated in accordance with administrative law. Based on the factors described above, the use of AI described in section 3.3.1 can therefore be placed on a gradual risk scale. This standardised location can then serve as a starting point for a specific assessment of how extensive the measures that the authority must take to ensure that AI supports compliance should be with the inquisitorial principle and/or the principles of administrative law regulating legal assessments of a discretionary nature.

3.4. *Summary and conclusion*

The assessment of the risk of a given use of AI can – in a Danish context – be placed at the above-outlined (graduate) scale as a starting point and be used to determine the degree of obligations as part of the good administration impact assessment, the testing procedures as well as implementation and monitoring measures. However, the potential risk cannot be determined solely via a standardised assessment based on the type of output the AI forms and the use thereof in public administration. As Danish administrative law tend to multi-factorial assessments, it will probably be advisable to supplement it with reflections on the differences between administrative areas and the affected group of citizens' case to case. In certain areas, the affected citizens will possess considerable expert insight themselves and have sufficient resources to verify and challenge any digitally generated output. It can, e.g., be well established companies in the environmental field. Thus, control will likely be strengthened by more frequent reviews by supervisory bodies and courts. In other areas such as asylum, social affairs, health and employment the affected group of citizens are generally in a more vulnerable situation.

4. *The AIA proposal*

On 21 April 2021, the European Commission presented a proposal for a Regulation on harmonised rules for AI. The purpose of the forthcoming regulation is to ensure a well-functioning internal market via harmonised regulation and ensure that AI in the EU is secure and respects existing legislation, fundamental rights and EU values and thereby make sure that Europeans can trust the AI they are using. At the same time, the proposal is to ensure legal clarity in order to promote investments in AI and thereby further innovation as well.[32]

Despite the fact that the proposal is still being negotiated, one must be able to assume that the forthcoming regulation will apply to the Danish public sector's use of AI. At the same time, the proposed risk-based approach is likely to stay, and the degree of compliance procedures and obligations will thus follow the (standardised) degree of risks, which the EU legislator (and later the EU Commission) determines to be associated with different uses of AI.[33]

The proposal, so far, divides into the following risk categories: 1) Unacceptable risk, where specific defined uses of AI are prohibited, 2) High risk, where there are specific requirements associated with certain uses, and where prior conformity assessments and subsequent market surveillance is required, 3) Limited risk, where there are transparency obligations associated with certain applications of the technology, and 4) low or minimal risk, where there are no specific requirements, but instead there is an opportunity to draw up voluntary codes of conduct to promote voluntary compliance with the requirements under the high-risk category. This classification is based on the intended purpose of the AI (as in product safety legislation). Thus, classification does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which it is to be used.[34] The proposed article 7 and the preamble number 28 indicates that the severity and extent of

[32] COM (2021) 206 Final, 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, 4, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. See further, e.g. E., Martin, Standardizing AI - The Case of the European Commission Proposal for an Artificial Intelligence Act, in L.A. DiMatteo, C. Poncibò, M.C. Cannarsa (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, Cambridge, Cambridge University Press, 2022 available at SSRN: https://ssrn.com/abstract=3900378 or http://dx.doi.org/10.2139/ssrn.3900378, visited 17 July 2022 or M. Veale, J.Z. Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach, in Computer Law Review International, vol. 22, 2021, 97.

[33] COM(2021) 206 final, section 5.2.2.

[34] COM(2021) 206 final, section 5.2.3.

potential harm on safety, health and fundamental rights of natural persons are the main criteria when the risks were (and will be in the future) assessed and scaled by the Commission.[35]

As the proposal is to be interpreted at the present stage, some of the AI systems used in the Danish public sector, as exemplified in section 3.2, will be regarded as high-risk systems. These include e.g. systems "intended to be used by or on behalf of public authorities to assess the eligibility of persons for public social services and services and to grant, reduce, cancel or revoke such services and services" in accordance with Article 6 of the proposal, cf. appendix 3, pkt. 5 (a). Here, regardless of how the negotiations proceed, it seems reasonably certain that the regulation will set up the type of regulation that here is referred to as compliance rules for these high-risk systems.

> In short, the AIA proposal contains a detailed regulation which entails comprehensive internal or external checks before high risk systems are implemented in the public administration. Further, providers have to implement a post-market monitoring system. Here, the similarities to the Danish administrative law will ease the implementation in the public administration, se above in sections 1-3.

On the other hand, the underlying risk assessments are somewhat different as Danish administrative law tend toward multi-factored assessments adapted to the national conditions. Therefore, some AI systems developed for and used in the Danish administration will – when the regulation enters into force – not be covered by the proposal's regulation on high-risk systems. As it is unlikely that deviant national regulation on risk categories and subsequent compliance regulation will be accepted, from a Danish perceptive a clash of legal cultures is approaching.

Depending on the outcome of the negotiations, challenges due to these discrepancies may be handled by incorporating existing Danish compliance regulation as codes of conduct according to Article 69 of the AIA proposal. This article provides – within some limitations – possibilities to extent and adjust the proposed high-risk regulation to AI systems not classified as such by the Commission. However, such use of codes of conduct will require a steady hand as over-implementation might result in disharmonious and ill-adapted requirements causing redundant bureaucratic exercises. Therefore, drafting such supplementary codes of conduct for public administration must be based on a solid systematisation of existing administrative law. Here, Danish jurisprudence may contribute and provide the basis for ensuring future coherence in the national legal system. However, as the Danish administrative law in its origins and core values has significant similarities with the other European legal systems, such research may also be extremely relevant in the other EU Member States.

[35] COM(2021) 206 final, section 5.2.3.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 113-124
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 09

Towards a New EU Regulatory Approach of the Digital Society *

Yves Poullet
(Emeritus Professor Faculty of Law, University of Namur, Co-chairman Namur Digital Institute)

ABSTRACT In recent times, the European Union has proactively multiplied the regulatory texts relating to various aspects of the digitalization of society. These texts take into account both the deep modifications of the digital market (merging of the telecommunications, audiovisual and information society services), the ubiquitous presence of certain actors and the increasing impact of our digital society not only on our way of doing business or conducting public affairs but also on our life and liberties. Through these texts, the Union's desire to chart a "Third Way" forward in terms of the development of our digital society, human centred, distinct from that of the United States and China and based in particular on respect for human rights . Beyond the multiplication of these texts, it is interesting to highlight a certain number of the characteristics of this EU regulatory approach: how the EU authorities have imposed a coregulatory model instead of self-regulation and how they are achieving a full consistent EU market. Furthermore, EU recent regulations adopt an asymmetrical approach in order to regulate especially the major actors and in order to ensure the proportionality of their intervention and the effectiveness of their regulations, the EU authorities promote a risk-based approach and of preventive measures, including the creation of internal compliance bodies, in addition to or instead of the traditional a posteriori legal control.

1. *Introduction*

The arrival of a new European Commission has resulted in a flurry of new regulatory texts in support of an increasingly proactive strategy to chart a third way for digital development. Artificial intelligence (AI for short), the *buzzword* of the advent of a digital society, has undoubtedly been the occasion for an intervention that goes far beyond the proposed AI regulation.

It is important to specify, first, this strategy that inspires Europe's regulatory action. At a time when regulatory projects are multiplying, the citizens of this Europe are wondering about the limits of this intervention by the European institutions. The issues of individual liberties, the attempts to democracy, the opening of our administrations, the health economy, the supervision of platforms, the regulation of new media against disinformation, etc. are all matters that the European regulator is concerned with.

A second point will detail the many facets of these projects, some of which are still open or simply envisaged.

The third point pinpoints the characteristics of digital texts in European legislation. The methods have changed. Gone are the days of directives and gone are the days of self-regulatory documents issued by the private sector. The European Union, including those advocating asymmetrical obligations about certain operators in the digital market, imposes detailed regulations. At the same time, there is a distrust of self-regulation and a concern for top-down co-regulation, which certainly leaves room for *soft law* but which is framed by numerous guidelines. A second feature is the creation and multiplication of administrative authorities at national level that are controlled or at least coordinated at European level. Anxious to ensure the proportionality of intervention and the effectiveness of regulations, we are seeing the emergence of a risk-based approach and of preventive measures, including the creation of internal compliance bodies, in addition to or instead of the traditional *a posteriori* legal control.

Finally, some reflections address the way in which the texts intend to ensure genuine European sovereignty, not hesitating to extend the application of these texts to companies located outside the territory of the European Union.

Before addressing these various points for the sake of completeness, I should have addressed the role of the Court of Justice of the European Union on the one hand, and of the Parliament, on the other, which is often a spur to the Commission's action. The multiplication of the Court's decisions is remarkable for its daring and innovative interpretation of regulatory texts, reinforcing them. The European Parliament's resolutions bear witness to the growing desire of this institution to play to the full its new assigned

* Article submitted to double-blind peer review.
The present text has been submitted in October 2022.

role of initiating and supporting the Commission's action. The limits of volume imposed on the present reflections constitute the only justification for our silence on their initiatives.

2. *The Objectives of a European Regulatory Policy for the Digital Society*

What specific regulatory response is Europe providing to the challenges of digital technology? Doesn't digital technology now stick to us, both figuratively and in reality? Does it not guide, for better or worse, our lives as well as those of companies and administrations? It is therefore important, and it is the role of the public authority, to map out the uses of a tool, which, increasingly, is the backbone of our economy, our society, our relationships, and ourselves. The introduction mentioned the European will to lead a third way. What is it about? This third way was undoubtedly prepared by the previous European Commission and the Parliament of the time, but it is now clearly affirmed by the famous "White Paper on Artificial Intelligence" published by the new Commission[1] and its President as soon as they took office. The strategy is explicitly stated in the White Paper and its implementation has since been carried out through texts that follow one another at an accelerated pace and go far beyond the issue of artificial intelligence.

As will be emphasised, it is a regulatory policy on data, its creation, use, transmission, and impact that Europe intends to develop in a coherent manner[2]). This is indeed a third way insofar as the European Union intends to conduct a digital development policy based on principles different from those that explain, on the one hand, the American policy which, no doubt wrongly, can be summarised as 'all for the market' and, more correctly, by the desire to maintain and develop the digital economy, on the one hand, by the desire to maintain and develop American leadership and, on the other hand, the Chinese policy marked - but we are probably close to a caricature - by State interventionism and an AI at the service of the economy, social governance by the State and the security of the latter to the detriment of the individual freedoms of citizens.

Europe intends to eliminate intra-European barriers to the deployment of AI and, more generally, digital technology. The clearly stated ambition is to enable the European Union "to compete with the massive investments made by third parties, notably the *United States*[3] and *China*".[4] [5]

The third path is based on the two terms used in the title of the White Paper on artificial intelligence: on the one hand, Excellence, which characterises the quality of applications and the research that supports their design, and on the other hand, Trust, which is necessary for the social acceptability of innovative digital developments, regardless of their field: education, health, mobility, public affairs, etc. It is a question of putting people at the centre of digital development and ensuring a solid framework for operators that allows for responsible innovation. Thus, "the Commission calls for a European society irrigated by digital solutions that are deeply rooted in our common values and that enrich the life of each one of us: citizens must have the possibility to develop themselves, to make choices in complete freedom and security, to

[1] European Commission, *White Paper on Artificial Intelligence - A European approach to excellence and trust*, COM (2020) 65 final 8, Brussels, 18 February 2020.

[2] Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions, *A European strategy for data*, COM/2020/66, Brussels, 19 February 2020, final: "The European data strategy aims to make the EU a leader in a data-driven society. Creating a single market for data will allow it to flow freely within the EU and cross sectors for the benefit of businesses, researchers, and public administrations. People, businesses, and organizations should be empowered to make better decisions based on insights from non-personal data, which should be available to all".

[3] www.usinenouvelle.com/etats-unis.

[4] www.usinenouvelle.com/chine.

[5] One weakness, however, that is often complained about is the level of European investment. In this respect, the figures quoted by the JRC report (M. Craglia (ed.), *Artificial Intelligence - A European perspective*, Publications Office of the European Union, Brussels, 3 December 2018, https://doi.org/10.2760/11251): "... United States, investments by GAFAM (private sector) and public authorities, DARPA (US Department of Defence Research Directorate: 7.5 billion dollars in 2020); China, for a volume of more than 20 billion; Europe (2.5 billion euros for 2018-2020), following the joint declaration of the Member States in April 2018 on their cooperation in the field of artificial intelligence Note the figures given in the *White Paper on artificial intelligence* (op. cit, 4): "However, the amount of investment in research and innovation in Europe remains well below the public and private investment in this field in other regions of the world. Some €3.2 billion was invested in AI in Europe in 2016, compared to about €12.1 billion in North America and €6.5 billion in Asia".

engage in society, regardless of their age, gender, or professional background. Businesses need a framework that allows them to start, grow, share, and use data, innovate, and compete or cooperate on a level playing field. And Europe must have the choice to pursue digital transformation on its own terms".[6]

This policy, which is particularly explicit about AI systems, seeks to reconcile respect for European ethical values without concealing the fact that this respect has an economic objective: i.e., the creation of a strong and sovereign European market, in particular through the creation of European labels or certificates (see *below*). As Ms Vestager emphasised when presenting the proposal for an "AI Act" Regulation, the aim of this text is to implement the very principles of excellence and trust: "In the field of artificial intelligence, trust is not a luxury but an absolute necessity. By adopting these landmark rules, the EU is taking the lead in setting new global standards that will ensure that AI is trustworthy. By setting the standards, we can pave the way for ethical technology worldwide, while preserving the EU's competitiveness. Future-proof and innovation-friendly, our rules will apply when strictly necessary: when the safety and fundamental rights of EU citizens are at stake".

The purpose of this major document is, according to the Commissioner, fourfold:

1) Ensure that AI systems placed on the EU market and used are safe and respect existing fundamental rights legislation and EU values;
2) ensuring legal certainty to facilitate investment and innovation in AI;
3) strengthen the governance and effective implementation of existing legislation on fundamental rights and safety requirements for AI system;
4) facilitate the development of a single market for legal, safe and trustworthy AI applications, and prevent market fragmentation.

This policy cannot be achieved without perfect coherence of the actions of all the member countries and presupposes both the drafting of more and more precise and numerous texts and better and better compliance, including by foreign companies offering digital products or services on European "territory". It considers the merging of three previously clearly distinct worlds: that of electronic communications, that of the media and that of Internet services.

3. *Themes - Multiplying and Expanding*

The traditional themes are addressed by new texts, either updating or broadening the regulatory concerns. As far as *digital service operators and operations are* concerned, the 1999 "electronic signature" directive has given way to the eIDAS Regulation No. 910/2014 of 23 July 2014, which aims to establish a common basis for secure electronic interactions between citizens, businesses, and public authorities, by setting up a framework for electronic identification and trust services. The increased attention to consumer protection has justified various texts consisting of a "New Deal for Consumers" Directive 2019/2061 of 27 November 2019 for a better application and modernisation of consumer protection rules and Directive 2020/1828 of 25 November 2020 on representative actions to protect the collective interests of consumers.

Directive 2009/770 on certain aspects of contracts for the provision of digital content or services is also noteworthy. This directive aims to fully harmonise the rules governing the conformity of digital content or a digital service with the contract, remedies in the event of lack of conformity or failure to supply and the way such remedies may be exercised, as well as the modification of digital content or a digital service.

The issue of the *protection of individual liberties* refers to the adoption of the RGPD, in place of Directive 95/47. The enshrinement of the Charter of Fundamental Rights of the European Union, adopted on 12 December 2007, allowed for a firmer European approach, broadening the rights of the persons concerned at the same time as it was important to address new issues, in particular profiling.

It is known that the 2002 directive on data protection in the electronic communications sector, known as *e-Privacy*, which was amended in 2009, is currently being revised as a regulation to adapt it to the protection requirements linked to the emerging

[6] European Commission, *Communication from the Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, *Shaping Europe's Digital Future,* COM(2020)67 final, Brussels, 1 February 2020, 2.

technologies of the Internet of Things and new communication services. Furthermore, the issue of access by law enforcement and judicial authorities to electronic evidence stored in the cloud awaits the adoption of the proposed Regulation on European orders for the production and preservation of electronic evidence in criminal matters.[7] In this respect, the European proposal, by forcing access to servers held by foreign companies, including in foreign territory, conflicts with the solutions of the American *Cloud Act* of 2018, which favours the law of the establishment of the operator of the *cloud* services, unless a treaty is concluded with the foreign country.

Freedom of expression and its abuses linked to violent or terrorist content of messages and disinformation, sometimes exacerbated by the pandemic, were the subject in May 2021 of "Guidelines" published by the Commission to reinforce the 2018[8] "Code of Practice on disinformation", but also of a proposal for a regulation, the "Digital Services Act", which proposes a regulatory framework for the provision of online services[9]. That proposal amends the famous provisions on liability of internet's hosting providers, contained within the directive on e-commerce dated from 2000, by extending the responsibility of information providers and overall, of platforms as regards the content disseminated through them.

The AVMS Directive 2018/1808 of 18 November 2018 determines, "taking into account *the evolution of market practices*", the minimum set of rules applicable in all EU Member States to audio-visual services including audio-visual product platforms and on-demand service operators. It promotes cultural diversity and regulates, inter alia, advertising, product placement, protection of minors, etc., and brings into the field of digital content regulation other authorities, namely the competent authorities.

It should be noted that this directive enshrines the disappearance of the social media or video-sharing services. It enshrines the principle of transparency of the operators of such services, regulates commercial communications and calls for appropriate national measures to protect young people and to combat violence and provocation to terrorism.

The fight against disinformation has been the subject of a "Guidance for strengthening the Code of practice on disinformation" and overall, the adoption of the *Digital Service Act,* Oct. the 19th of 2022. In addition, the fight against electronic terrorist messages was the subject of Regulation 2021/784 of 29 April 2021 on combating the dissemination of terrorist content online.

All these texts aim to "improve the functioning of the digital single market by enhancing legal certainty for hosting service providers and user confidence in the online environment, as well as guarantees for freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society, and media freedom and pluralism". They propose a control of the technological tools used to filter messages for their content or even to audit them, oblige at least some operators to set up human moderation and mediation bodies, and ultimately the possibility of recourse to the courts.

As for *intellectual property*, the same reference to technological developments justifies the adoption of Directive 2019/790 on copyright and related rights in the digital single market on 17 April 2019. The Directive "provides for rules to adapt certain exceptions and limitations to copyright and related rights to the digital and cross-border environment, as well as measures to facilitate certain licensing practices, including, but not limited to, the dissemination of commercially unavailable works and other subject-matter and the online availability of audio-visual works on video-on-demand platforms, with a view to ensuring wider access to content. It also contains rules

[7] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European orders for the production and preservation of electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council establishing harmonised rules on the appointment of legal representatives for the purpose of obtaining evidence in criminal matters*, n° 6946/19, Brussels, 28 February 2019.

[8] European Commission, *Guidance on Strengthening the Code of Practice on Disinformation*, COM(2021) 262 final, Brussels, 26 May 2021.

[9] On 15 December 2020, the European Commission presented its proposal for a regulation to regulate the digital single market: the *Digital Service Act*. This first proposal aims to provide a harmonised framework of rules for online services, mainly in terms of moderation of illegal content and transparency of service. This proposal distinguishes rules according to various categories of operators, from simple web services to very large platforms. See also, the Proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Ac), Brussels 16.09.2022, COM(2022) 457 final, still in discussion.

to facilitate the use of content which is in the public domain. In order to achieve an efficient and fair market for copyright, there should also be rules on rights in publications, on the use of works or other subject matter by online service providers who store and provide access to content uploaded by their users, on the transparency of 'authors and performers' contracts and on the remuneration of such authors and performers, as well as a mechanism for revoking rights which authors and performers have transferred on an exclusive basis".

Beyond this intervention in traditional areas, the European Union has addressed regulations to communication infrastructures, to the technology itself and to some of its products. About infrastructures, in terms of technology, cybersecurity has become a major issue in European policy. It is the subject of a Regulation 2019//881 of 17 April 2019 "on ENISA (European Union Agency for Cyber Security) and on Information and Communication Technologies Cybersecurity Certification".[10] With regard to products, without being exhaustive, it should be noted that the intelligent car is the subject of regulatory texts.

Regulation 2017/745, which the case law of the Court of Justice now extends to telemedicine software and AI applications in the health field, succeeded the Medical Devices Directive.

Then, finally, AI technologies, which are applicable in many areas, are the subject of a Commission proposal for a Regulation known as the "AI Act".[11] This proposal aims to provide a framework for the development of artificial intelligence applications, by distinguishing various categories based on an analysis of the risks associated with these applications. For so-called high-risk applications, it intends to establish both internal governance and a risk assessment procedure on the model of the Regulation on medical devices, including external evaluation by a supervisory authority including external assessment by a supervisory authority, maintenance of a register and European certificates of certificates of conformity. On the subject of robots, which often incorporate AI systems, the Commission is proposing, on the same day as its AI proposal, to replace the 2006 Machinery Directive by a new regulation on machinery and equipment[12] targeting notably robots, 3D printers, intelligent lawnmowers or cars. This new regulation will be better able to ensure integration of AI systems while reducing administrative burdens and costs through simplified through simplified procedures.

It should be added that the texts relating to AI refer to others that respond to the European strategy of creating a European data market and, at the same time, augur the possibility of setting up European *big data*, capable of feeding AI systems. As part of this policy of increased data circulation and sharing, the Commission has taken various initiatives. Recently, the Data Act[13] proposal intends to favour the data sharing as regards the data collected by Internet of things technologies, and that among all actors including the public sector, ensuring a functional interoperability between information systems, and excluding any "sui generis" right to the data base resulting from the collection of the data generated using the devices.

The main one is certainly the proposal for a regulation on European data governance (*Data Governance Act*) presented on 25 November 2020,[14] which encourages, through the creation of regulated services known as data sharing, the sharing of data not only between companies but also between the private and public sectors, and even between individuals and the public sector, with regard

[10] See, about 5G, NIS Cooperation Group, *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, CG Publication, 2020 and about connected cars, Consolidated text: Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, OJ L.151 14.6.2018,1 and ff. amended by the Commission delegated regulation 2021/1445, 23.06.2021, O.J. L. 313, 4 and ff.

[11] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence legislation and amending certain Union legislative acts* COM(2021*)*, Brussels, 21 April 2021, 206, final {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}.

[12] COM(2021) 202 final, Brussels, 21 April 2021.

[13] Proposal for a regulation on harmonized rules on fair access to and use of data, Brussels 23. 2. 2023, COM(2022)68 final.

[14] European Commission*, Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM(2020) 767 final, 2020/0340(COD), Brussels, 25 November 2020.

to "Data for public Good", within the framework of *data altruism*.

As far as the public sector is concerned, Europe is promoting the widest possible exploitation of public sector data by the private sector. In this respect, no sooner has the ink dried on the 2019 *Open Data* Directive,[15] which already significantly strengthens the obligations to make available information held by the public sector, than the proposed Data Governance Regulation of 25 November 2020[16] expands these obligations in one further aspect, namely, to open the re-use of protected data previously excluded from access.

Lastly, the European Union is paying particular attention to the regulatory framework for certain operators, the *very large platforms, which are* now described as the *gatekeepers* of the information society. In this respect, through their recommendation and profiling systems, they generate so-called 'systemic' risks, according to the definition given in the draft DSA, i.e. in addition to the impact on our individual freedoms; they also have an impact on the democratic functioning of our society and on social justice. The market share occupied by these companies and their strategy of diversification of activities profoundly de-structure the boundaries hitherto drawn by regulation between audio-visual services and digital services, such as functioning of the competitive market and oblige the European Union to intervene. This is the purpose of both the Regulation of 20 June 2019 "promoting fairness and transparency for business users of online intermediation services" and, more recently, the enactment of the *Digital Market Act*, which introduces asymmetric regulation of information service operators,[17] taking into account their importance on the market and therefore, their possibility to disturb a fair competition by giving advantages to their own subsidiaries or affiliates or by manipulating their customers by merging different data bases[18].

Furthermore, it should be noted that the Electronic Communications Code, since its revision in 2018,[19] now includes providers of so-called OTT (over-the-top) communication services, providers of instant messaging services, emails, telephone calls on the Internet and social networks, in the definition of electronic communications operators. They are therefore subject to the same obligations as "traditional" operators, in particular as regards interoperability, information and protection of end-users, public security and national defence, and even the financing of the universal service, and to specific rules on the protection of privacy.

Advanced technologies are indeed merging the previously separate markets of traditional electronic communications operators on the one hand and communications platforms such as What's App on the other. As noted in Recital 7 of the Directive, the convergence of the telecommunications, media and information technology sectors implies that all electronic communications networks and services should be subject as far as possible to a single European electronic communications code established by means of a single directive.

4. *Towards Original Modes of Regulation*

4.1. *Regulations instead of Directives*

What can we learn from this efflorescence of European texts? In what way do they mark an evolution in the European Union's modes of regulation? There are several points to be made in this respect: the first is the proliferation of regulations, whereas until recently Europe was content with directives. The example of the passage from the 1995 directive on data protection, which, according to the very terms of its recitals, left room for manoeuvre to the Member States, has given way to a regulation that not only imposes common rules but also creates the bodies for

[15] See Directive 2019/1024/EU of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, O.J.E., L 172, 20 June 2019, available online at: https://op.europa.eu/en/publication-detail/-/publication/a6ef4c41-97eb-11e9-9369-01aa75ed71a1/language-fr/format-PDFA2A. The proposal was adopted with minor amendments by the Committee on Industry, Research and Energy on 16 July 2021.

[16] COM (2020) 767 final.

[17] 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), Sept, the 14th, 2022. The Digital Markets Act introduces a new regulatory model based on a system of graduated obligations, known as "asymmetric", which adequately targets the largest players.

[18] The Data Act proposal (article 5.2) forbids that the "gatekeepers" shall be third party as regards the sharing of data generated by using IoT systems.

[19] Directive (EU) 2018/1972 of 11 December 2018. This directive replaces five directives.

maintaining and even amplifying this consistency.

No doubt there are still relays at national level (data protection and audio-visual control authorities, supervisory bodies for AI, etc.) whose powers of investigation and sanction have been strengthened, but these national authorities are forced to work in close cooperation and are even controlled by so-called European coordination bodies at European level.

4.2. *The proliferation of independent administrative authorities*

Several texts thus create European agencies or authorities responsible for ensuring the coherence of the actions of national authorities and for ensuring the uniform interpretation and application of texts. These authorities express themselves through "guidelines", recommendations, opinions, and reports and advise the Commission in its regulatory work. Without being exhaustive, let us mention: the EDPB in the field of data protection, ENISA in the field of cybersecurity, the Medical Devices Coordination Group, the European Artificial Intelligence Committee, the European Regulators Group for Audio-visual Media Services (ERGA), BEREC (Body of European Regulators for Electronic Communications) or in French, ORECE, which provides administrative and professional support to the European Commission.[20] AI and Data Act proposals are in the same way considering the setting up of national independent supervisory authorities.

With the same concern and to further increase the effectiveness of the regulatory texts and ensure their rapid adaptation to the needs of technological development, the texts also confer powers on the Commission, either to monitor the application of the regulations in the form of reports in particular, or to adopt delegated acts pursuant to the text of the Regulation. Thus, to take the examples of the "AI Act": reviewing the scope of the AI Regulation, completing the list of high-risk systems, etc.

It should be noted that when the Commission is directly responsible for implementing the provisions of a European competence such as, in competition, the texts adopted in these areas such as the DMA, the Commission, assisted by an Advisory Committee on Digital Markets made up of representatives of the various member countries, can directly impose binding measures on companies.

The proliferation of administrative authorities created by all these recent texts raises difficulties when it comes to analysing the impact of a technology in a cross-cutting manner or to giving a ruling in a dispute that involves the various issues considered separately in the regulatory framework and by bodies with different cultures and prerogatives. To take the example of the use of recommendation and profiling systems by digital platforms, this is an issue that touches on data protection, freedom of expression and media regulation, competition, and consumer protection.[21]

This need for a cross-cutting approach can, in our opinion, only be met by clarifying the role and competences of each category of administrative authorities but, above all, by institutionalising the creation of forums for dialogue between these different bodies, without which there is a risk of contradictory interventions or even rivalry between authorities.

It is worth noting, in connection with the designation of the proposed national supervisory bodies for AI, that data protection authorities have asked to assume this competence, even though data protection issues are only part of the risks to be considered when assessing AI systems. This is

[20] "BEREC aims at fostering the independent, consistent and high-quality regulation of digital markets for the benefit of Europe and its citizens". (BEREC strategy 2021-2025). Directive (EU) 2018/1972 of 11 December 2018 confers a significant number of new tasks on BEREC "such as issuing guidelines on several topics, reporting on technical matters, keeping registers, lists or databases and delivering opinions on internal market procedures for draft national measures on market regulation. Overall, the EECC aims to create an internal market for electronic communications within the EU while ensuring a high level of investment, innovation, and consumer protection through enhanced competition". National regulatory authorities and the Commission should take the utmost account of the recommendations, guidelines and best practices adopted by BEREC (Recital 21 of the Electronic Communications Services Directive). BEREC works to ensure that European legislation is applied in a uniform manner, so as to enable the EU to have an effective single market in electronic communications. It provides advice, on request and on its own initiative, to the EU institutions. It consists of a Board of Regulators. This is a body composed of the heads (or high-level representatives) of each national regulatory authority.

[21] Another example is the regulation of connected cars, which involves questions of infrastructure choice (5G or WiFi), data protection, interoperability, and security standards.

probably one of the first initiatives to regulate a technology across the board. An example to follow?

4.3 *Coregulation under control*

Finally, it is emphasised that the convergence of previously distinct sectors such as the worlds of telecommunications, audio-visual and e-commerce services now requires online platforms in particular to juggle regulations from different cultures, which are applied cumulatively and, it is hoped, coherently in their own right. Europe's desire to achieve its objectives explains the regulatory approach and its mistrust of self-regulation, which is difficult to control and above all the prerogative of the powerful. This attitude is not in contradiction with the forms of co-regulation that we have described in previous texts as top-down, i.e. private regulatory mechanisms are certainly promoted but severely framed by a regulation that sets the guidelines and even controlled by the independent administrative authorities set up and even by the Commission itself.[22]

This trend is reflected in many texts and, sometimes, explicitly, as in these recitals (See recitals 12 and 14 translated by Article 4a) of the Audio-visual Services Directive: "Member States should, in accordance with their different legal traditions, recognise the role that effective self-regulation can play as a complement to existing legislative, judicial and administrative mechanisms, as well as the usefulness of its contribution to the achievement of the objectives of Directive 2010/13/EU. However, while self-regulation can be a complementary method of implementing certain provisions of Directive 2010/13/EU, it should not be allowed to replace the obligations of the national legislator. Co-regulation, in its simplest form, provides a legal link between self-regulation and the national legislator, while respecting the legal traditions of the Member States. In co-regulation, the role of regulator is shared between the stakeholders and the public authorities or national regulatory authorities and bodies. The role of the competent public authorities includes the recognition of the co-regulatory system, the audit of its procedures and its financing. The possibility of state intervention should exist, within the framework of co-regulation, when the objectives of the system are not met…". It is illustrated by the way in which, as regards disinformation, after having accepted in 2018 self-regulation by the major market players, in addition to the launch of the DSA proposal already studied, the Commission published on 26 May 2021 - the title is evocative - the "Guidelines for strengthening the Code of Conduct on misinformation".[23]

Without being exhaustive, we can mention in the same vein the articles 40 et seq. of the GDPR, which, while recognising various methods of private regulation (codes of conduct, labels, certificates), set minimum conditions for them and provide for their approval by DPAs.[24] The "AI Act" allows for self-regulation but only for low-risk AI applications. It should be noted that the European authorities insist on *multi-stakeholder* participation in the drafting of self-regulatory instruments.[25]

It should be added that this same concern to bring private regulation into line with the requirements of public regulation is also expressed in relation to another mode of regulation: technology, the operation of which imposes what many authors (see Reidenberg, Trudel or Lessig) have called the *lex informatica or electronica*. It is important that the *design of* technological tools and their applications conform to the rule of law from the outset. A number of European texts require designers or users to comply with the

[22] For a fuller account of the relationship between European regulation, self-regulation and the "lex informatica", see Y. Poullet, *Vues de Bruxelles. Modes alternatifs de régulation et libertés dans la société du numérique*, in C. Castets-Renard, V. Ndior et L. Rass-Masson (eds.), *Enjeux internationaux des activités numériques*, Brussels, Larcier, 2020, 91-137.

[23] "The Guidance aims at evolving the existing Code of Practice towards a co-regulatory instrument foreseen under the Digital Services Act (DSA), offering an early opportunity to design appropriate measures to address systemic risks related to disinformation stemming from the functioning and use made of the platforms services in view of the anticipated DSA risk assessment and mitigation framework".

[24] On this point, the policy followed by DPAs, *Guidelines 1/2019 on codes of conduct and monitoring bodies under Regulation (EU) 2016/679*, 4 June 2019.

[25] Among many examples, we can cite the injunction on 2 of the "Guidance for strengthening the code of Practice on disinformation": "Online platforms and all other players of the online advertising ecosystem should thus take responsibility and work together to defund disinformation. (See, in particular, the creation by the 'Guidances' of the European Digital Media Observatory, which includes researchers, representatives of 'fast-checkers' and other 'relevant stakeholders".

law: for example, the GDPR puts forward the principle of "privacy by design" (Article 25); the 2018 Copyright Directive insists that the control systems used to combat illicit copying respect the law's exceptions (Article 17.7); the DSA proposal (Article 28) requires the verification of recommendation systems and we will come back to the "AI Act" proposal which, beyond the "Privacy by design" of the GDPR, advocates "Ethical values by design".[26]

4.4. *Asymmetrical regulation of the players*

Another characteristic seems to be emerging in the most recent European Union texts, namely asymmetrical regulation of both the players and the applications operated, or products or services offered by them, depending on the risks (*risk-based approach*) associated with these applications, products or services. In both cases, the regulatory asymmetry is justified by the principle of proportionality, affirmed by Article 5(4) of the Treaty on European Union, which stipulates that the Union must not in exercising its powers do more than is necessary to achieve its objectives. Let us look at these two points in more detail.

Some European regulations impose heavier obligations on certain categories of actors. For others, they grant exceptions to facilitate their development. The second chapter (*supra,* no 10) already pointed to certain provisions imposed on communication and information platforms, such as the equal and transparent treatment of professional users by these necessary intermediaries. Similarly, the DSA imposed obligations on *very large platforms* (i.e. those with a customer base equal to or greater than 10% of the European population) to monitor content and audit recommendation systems.

At the other end of the spectrum, there is a desire to protect research organisations, start-ups and even SMEs in order to guarantee innovation. Thus, Articles 3 and 4 of the 2019 directive on the protection of intellectual property provide scientific research bodies with the exceptional right to carry out data searches, notwithstanding the sui generis or intellectual property rights of right holders or their successors. The same concern can be found in the texts relating to access to public data and data sharing. Similarly, Article 55 of the *IA Act* provides for the possibility of national measures "in favour of small providers and users".

It is known that the 2019 European Regulation promoting fairness and transparency for businesses using online intermediation services is fully justified by this desire to protect SMEs[27] and that the intermediation services envisaged under the *Governance Data Act* proposal are intended to assist SMEs to benefit from the advantages of data sharing. More recently, the Data Act proposal is protecting under the common concept of "user" both individuals and legal persons by affording the same data protection including the rights to access, to be informed and to consent to the sharing of the data generated by their use of IoT devices.

Finally, Article 17.6 of the 2019 Copyright Directive exempts from certain due diligence obligations "new providers of online content sharing services whose services have been publicly available in the Union for less than three years and which have an annual turnover of less than EUR 10 million calculated in accordance with Commission Recommendation 2003/361/EC (which defines SMEs)".[28]

4.5. *The 'risk approach'*

The genuine risk-based approach leads to the creation of new obligations when certain criteria proposed by the regulation indicate

[26] In addition to compliance with the Law, the European Commission's May 2019 statement, following the recommendations of the expert group, AI applications should not only be consistent with the Law but also adhere to ethical principles.

[27] "Online intermediation services can be critical to the commercial success of businesses that use them to connect with consumers. To take full advantage of the online platform economy, it is therefore important that businesses can rely on the online intermediation services with which they enter a commercial relationship. This is important mainly because the increasing intermediation of transactions through online intermediation services, because of significant indirect data-based network effects, leads to an increased dependence of these user enterprises, in particular micro, small and medium-sized enterprises (hereinafter referred to as "SMEs"), on these services to contact consumers" (Recital 2).

[28] In paragraph 2 of the same article, a second criterion is added to qualify the application of the first: "Where the average number of unique visitors per month of such service providers exceeds 5 million, calculated on the basis of the previous calendar year, they shall also be required to demonstrate that they have used their best efforts to avoid further uploads of the works and other protected subject matter covered by the notification for which the rightsholders have provided the relevant and necessary information".

that higher risks are present. This approach is already used, but in a very limited way, in the provisions of the GDPR: Article 35 reserves the obligation to carry out an impact assessment only to processing operations presenting a "high risk" to the rights and freedoms of natural persons. The notion of "high risk" remains unclear. The Regulation on medical devices similarly distinguishes between different classes of products and services according to the purpose of their use and the risks related to health and safety, and subjects "high risk" classes of products to conformity assessment procedures.

The same idea runs through the "AI ACT". The proposal sets out the prohibition of illegal practices of artificial intelligence[29] (Art. 5); it establishes a system of control and management of high-risk AI systems (Art. 6.2) listed in an annex that may be amended by the Commission; it imposes specific obligations for lack of transparency on certain hidden applications "in particular when ultra-realistic dialogue or video tricks are used"; and, finally, it leaves other applications presenting a minimal risk to the self-regulation of the market. The "AI Act", or rather the work of the *High-Level Group of Experts on AI* on the ethics of AI,[30] to which this proposal constantly refers, broadens the risks to be taken into consideration when assessing AI applications. Thus, in addition to the risks to our individual freedoms, there is the need to take into consideration the so-called collective risks specific to a group of people or not, the risks of undermining social justice and, beyond that, the societal risks, such as those to the environment, democracy, and respect for the rule of law. This broadening is reflected in the definition of "systemic risks" linked to the operation of rating and recommendation systems and their use by "very large platforms".[31] We know that the first works on the liability of AI systems[32] retain the same idea of differentiating the responsibilities of the "producers" or professional users of AI systems according to the seriousness of the damage that the use of the systems may cause.

Another consequence of the risk-based approach is that it fully justifies the shift from a classic legal drafting - based on the definition of behavioural content to be respected and, in the event of non-compliance, on the repression or *a posteriori* sanctioning of breaches of the regulations - to an *a priori* approach based on the obligation to assess risks, i.e. to set up a risk assessment procedure and monitor compliance with this procedure. The preventive risk-based approach seems to be a characteristic of recent European regulations. The example already cited of the "Privacy Impact Assessment", introduced by the GDPR, thus shifts the scope of intervention of the regulation towards a preventive approach of risk avoidance by the need to set up an assessment procedure at the design stage of the processing. The same idea runs through the other regulations mentioned in the previous paragraph. In particular, the proposed "IA Act" develops this procedure at leisure, defining its stages, its content, insisting on the participation of all the interested parties, etc. This approach is to be commended, although it is administratively more cumbersome and can only be justified in cases of significant risk.

4.6. *Towards more effective regulations*

Chapter 1 emphasised *in fine* the Union's concern to ensure the effectiveness of

[29] For example, subliminal message manipulation systems, the exploitation of vulnerabilities, the use by the public sector of "social ranking" systems leading to potential discrimination between individuals or groups, biometric systems operating in real time and remotely, placed in public places (e.g. facial recognition systems).

[30] High-Level Expert Group on AI (HLGE), *Ethical guidelines for trustworthy AI*, 8 April 2019, No. 67, text available at: Ethics guidelines for trustworthy AI - Publications Office of the EU (europa.eu).

[31] Recital 57 of the DSA describes these so-called risks. The first concerns the extent to which online platforms with a significant market share can disseminate illegal content. The second concerns "the impact of the service on the exercise of fundamental rights, as protected by the Charter of Fundamental Rights, including freedom of expression and information, the right to privacy, the right to non-discrimination and the rights of the child. Such risks may arise, for example, from the design of the algorithmic systems used by the very large online platform or from the misuse of its services through the submission of abusive notifications or other methods aimed at preventing freedom of expression or hindering competition". The third risk is the use of mechanisms put in place by the platform, such as the recommendation system, to manipulate others in elections, to spread intentionally wrong messages that endanger public health, democracy, etc.

[32] European Commission, *Liability for Artificial Intelligence and other emerging digital technologies*, Report of the Expert Group on Liability and New Technologies, Section on New Technologies, Brussels, 21 November 2019. The European Commission seems to want to take up the ideas of this proposal for a regulation through a profound modification of the 1985 Directive on liability for defective products.

regulation, i.e. to guarantee compliance. The preceding paragraphs have already illustrated the way in which the Union intends to respond to this concern, by bringing self-regulation into line, by translating regulatory prescriptions into technology, by the role of the administrative authorities, not forgetting regular monitoring by the European Commission. One point must be added: the imposition of internal *compliance* mechanisms. The GDPR imposes (Article 37 et seq.) the obligation for certain companies to appoint a data protection officer, who enjoys a status that ensures a certain protection and has numerous competences and missions to ensure compliance with the GDPR. Other texts have since joined this idea. Thus, the so-called DSA proposal obliges, on the one hand, platforms to set up internal complaint handling systems, responsible for ensuring the legality of decisions taken automatically or not by the platform and, on the other hand, very large platforms to appoint one or more compliance officers.[33] Article 15 of the Medical Devices Regulations 2017 provides that "manufacturers shall have at least one compliance officer within their organisation with the requisite expertise in the field of medical devices".

4.7. *The EU "sovereignty" in the global digital space*

Finally, we shall mention the European determination to fully exercise its sovereignty in the digital space, not by creating technical gateways as notably Russia and China but by using the legislative tools and by ensuring their full effectiveness. This sovereignty implies, on the one hand, the extension of European rules to companies located outside Europe but also, on the other hand, the presence on the European market of products or services that comply with these regulations. The first facet of this sovereignty, i.e "control of our destiny on the computer networks",[34] is the trust and values of the European Union.[35] The trust and values of the European Union, which are reflected in the regulatory texts, can only be guaranteed and respected to the extent that, in a global digital market, the services and products using artificial intelligence and deployed on European territory effectively comply with the requirements of European regulations. It is on the basis of this premise that, in particular, the GDPR (art. 3) and the proposed regulation on AI or digital services do not hesitate to extend their scope of application to companies located outside the European Union when the processing, AI application or digital service is aimed at a clientele located in the European Union or when the application or product is intended for the European[36] market or residents. This broadening of the scope *ratione loci* of the European texts reflects the European will to use the regulatory tool to guarantee the protection of persons residing in Europe and, consequently, their trust in the AI tool developed or used there. Beyond that, it is an attempt to export the European regulatory model, insofar as the penetration of the European space by companies located outside Europe obliges them to obey the rules that prevail there and invites them to avail themselves of the added value of these rules with regard to all their markets. The same idea of sovereignty is reflected in the proposed "e-evidence Act", which allows police and judicial authorities to request data stored

[33] Article 32.2: "Very large online platforms shall only appoint, as compliance officers, persons who have the professional qualifications, knowledge, experience and skills necessary to carry out the tasks referred to in paragraph…".

[34] www.lepoint.fr/politique/emmanuel-berretta/la-souverainete-numerique-ce-dossier-qui-effraie-hollande-et-valls-13-01-2016-2009389_1897.php.

[35] On digital sovereignty, read, among others, the excellent contribution of A.T. Norodom, *Être ou ne pas être souverain, en droit, à l'ère numérique*, in *Enjeux internationaux des activités numériques*, C. Castets-Renard, V. Ndior et L. Rass-Masson (eds.), Brussels, Larcier, 2020, 21 and ff.

[36] The argument is noted in several regulations and proposed regulations, such as the RGPD, the AI proposals, the DSA... Among all these texts, let us simply quote: "As online intermediation services and search engines have a global dimension, this Regulation should apply to providers of such services, whether they are established in a Member State or outside the Union, provided that two cumulative conditions are met. The first is that business users or users of business websites should be established in the Union. The second is that the business users or users of business websites should offer, through the provision of these services, their goods or services to consumers located in the Union for at least part of the transaction. In order to determine whether business users or users of business websites offer goods or services to consumers located in the Union, it is necessary to determine whether it is obvious that business users or users of business websites direct their activities towards consumers located in one or more Member States" (Explanatory Memorandum, point 9 of the Regulation of the European Parliament and of the Council promoting fairness and transparency for business users of online intermediation services, adopted on 14 June 2019 (OJEU, L.186, 11 July 2019, 57-79).

outside Europe from companies based outside Europe when fighting certain serious crimes.
The requirement of sovereignty also implies, as a second facet of the Union's sovereignty over the digital space, the promotion of products or services that comply with European requirements. Indirectly, the measure aims to encourage the development of a digital products and services industry. Several texts thus set up European certificates which allow companies that use them to be presumed to meet the regulatory requirements and citizens to have a reassuring quality label. The GDPR provides for this possibility in the context of co-regulation. An EU Trust Mark is established for certification trust service operators under the eIDAS Regulation. The 2019 Cybersecurity Regulation establishes a system of voluntary certification to ENISA of products, services or procedures related to their security under certification schemes adopted by the Commission.[37] The regulations on medical devices and on AI represent a step forward in this area insofar as, including for foreign importers, they prescribe, at least for systems or devices presenting a higher risk, this obligation to be certified internally or, exceptionally, by an approved notification body, organise the quality control of the certification by a supervisory body and, finally, organise a European register of such certificates. These certification systems are a major challenge for the creation of a European market for products and services that comply with regulatory requirements and the promotion of European players on this market, with the hope that these certificates can also be an added value on export markets.

5. *Conclusion*

Our contribution aims to highlight this pervasiveness of European regulation. The erasure of borders due to the creation of a universal digital space does not mean the free pass that the Net superpowers dream to impose their own regulation through self-regulation and more insidiously by technological options. The European Union does not intend to reinstall the barriers or, at least, the filters that certain powers such as China or Russia surround their national spaces with, but at least to subject the entry into the lives of European citizens, companies and administrations to a certain number of precautions which, as we have seen, go well beyond the sole concern of data protection and individual freedoms to extend to the protection of our European democratic societies and the values of social justice. In the name of these values, it is asserting and even imposing - some would say imperialistically - its regulatory choices and leaving behind the defensive culture that has often been its own. To do this, it puts a damper on the principle of subsidiarity and refuses the profusion of national texts whose impact would have been insufficient to combat the dangers of an area which would otherwise have obeyed the law of the strongest or the 'lowest bidder' country. The challenge of “excellence and trust” can only be met together. To this end, the Union is adopting texts that are undoubtedly far removed from traditional approaches; it is multiplying the links between law and technology to ensure compliance with the former; it is forcing certain cultures, such as that of property by encouraging data sharing, that of an administration that is jealous of its secrets and its data, and that of administrative authorities that are jealous of their traditional competences and prerogatives.
The regulation of the Union of our digital society opens vast areas for us lawyers and, no doubt, new ways of doing things for a better society.

[37] See Articles 46 *et seq*. of the Regulation of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on cybersecurity certification of information and communication technologies: “1 The European Cybersecurity Certification Framework is hereby established in order to improve the conditions for the functioning of the internal market by enhancing the level of cybersecurity within the Union and by providing a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes. 2 The European Cybersecurity Certification Framework shall provide a mechanism to establish European cybersecurity certification schemes and to attest that ICT products, ICT services and ICT processes that have been assessed in accordance with these schemes meet defined security requirements, with the aim of protecting the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed or the functions or services that are offered by or accessible through these products, services and processes throughout their life cycle”.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 125-129
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 10

*Is the European Union Thinking About a Charter of (Fundamental) Digital Rights?**

Patrizia De Pasquale
(Full Professor of EU Law at the Federico II University of Naples)

ABSTRACT Even if certain situations concerning the digital society may fall within the scope of rights recognised by the CFREU, given their broad formulation, the approval of an "European Union Charter of Digital Rights" seems the best solution to protect digital rights nowadays. This Charter would be a useful tool to define the system of rights protection in a more sophisticated and up-to-date way, offering the Court of Justice a precise benchmark.

1. *Introduction*

The constant acceleration to which technological evolution is subject and its unpredictable nature call into question the adequacy of the traditional instruments to protect digital rights. An assessment of the level of guarantees provided by the European Union and a reflection on the important role that the Charter of Fundamental Rights (henceforth "the Charter" or "CFREU") is called upon to play in this context therefore seems necessary. On the contrary, it seems appropriate to ask whether a broad reading of the Charter is sufficient to guarantee full protection of these rights, in view of the rapidity with which new technological breakthroughs are taking place and the peculiar situations that determine.[1]

In fact, the adoption of the recent Communication on establishing a European Declaration on Digital Rights and Principles casts doubt on the suitability of the CFREU alone to cover the (expanding and in many ways unknown) universe of such rights.[2]

It seems that the Commission is moving towards the elaboration of a catalogue of digital rights, starting to test the ground and, therefore, the willingness of Member States to proceed in that direction, through acts of soft law. In fact, it is expressly stated in the Communication that the Declaration is without prejudice to the protection of the rights of persons online ensured by the Union's legal framework through the well-known judicial remedies. Nevertheless, "other [rights] may require further action, at the appropriate level".[3]

Indeed, certain situations concerning the digital society may fall within the scope of rights recognised by the CFREU, given their broad formulation - think, for instance, of the protection ensured to dignity, health and family life, which can be included without too much effort in the rights of the digital age[4] - but others will have to find an appropriate place in the EU's primary provisions in order to avoid a mere hermeneutic operation turning into a *deminutio capitis*.

The drafting of further legislative instruments could create excessive confusion in coordination and interpretation, but the

* Article submitted to double-blind peer review.

[1] See A. Adinolfi, *L'Unione europea dinnanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (ed.), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, Pacini Giuridica, 2020, 13.

[2] 26 January 2022, COM/2022/27; for the text of the Declaration, see European Declaration on Digital Rights and Principles for the Digital Decade, 2023/C 23/01, PUB/2023/89, 23 January 2023, available in eur-lex.europa.eu. For an early comment, see E. Celeste, *Towards a European Declaration on Digital Rights and Principles: Guidelines for the Digital Decade*, in *dcubrexitinstitute.eu*, 7 February 2022.

[3] COM/2022/27, cit., para 4.

[4] The Court of Justice has already been able to assess the impact of internet use on certain rights, albeit not strictly "digital". For example, it has recognised and protected the right to be forgotten and, with two judgments in 2019, set territorial limits to its exercise or rather "de-indexing" (judgments of 8 April 2014, joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*; 13 May 2014, case C-131/12, *Google Spain*; 6 October 2015, case C-362/14, *Schrems (Facebook)*; 24 September 2019, case C-507/17, *Google CNIL*; 3 October 2019, case C-18/18, *Glawischnig-Piesczek*. See O. Pollicino, *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *federalismi.it*, No. 19, 2019, 2.

absence of *ad hoc* provisions would have even more serious consequences, resulting in a failure to recognise the complexity of the "digital world" and in extremely serious discriminatory situations.

The simplest solution, at least theoretically, is obvious: approve a "European Union Charter of Digital Rights" that would constitute a parameter of legitimacy of Union acts and guarantee effective protection of these rights. Alternatively, and only if this option were not feasible, then some substantial amendments to the existing Charter could be introduced, adding to the various articles a precise reference to the "digital" and its implications for the specific right covered.

However, the path taken by the Union with regard to digital rights is no less arduous than the one it took at the time to arrive at the approval of the Charter of Fundamental Rights and which - as is well known - involved a series of intermediate stages.[5] The need for a Union Charter of Digital Rights, however, clashes with Member States' resistance to its contents.

In fact, also at the national level, the great revolution induced by the Internet in everyday life is at the center of the debate and has led to the adoption of a plethora of provisions, which see the public administration as the main protagonist and which find in the internal dimension the easiest place to plan strategies to govern such phenomena.

Hence, the EU Charter of Digital Rights - as has already happened with its counterpart - would be born as a "superstructure" with respect to the national rules, stratified over time; to which would be added the rights that, at the time of its adoption, will be brand new. More precisely, its function would not only be to innovate, but also to make explicit a series of principles and rights that, in the meantime, the Court of Justice will have already guaranteed in case law, thanks to a complex operation based mainly on analogy juris.

Beyond the difficulties connected with the coordination of similar rules, this catalogue would, in any case, give an acceleration towards European digital citizenship, providing Union citizens with easy access to digital public services, on the basis of a universal digital identity, as well as to digital health services. In other words, it would send a clear signal towards the full recognition of a Union legal space in which rights and duties can be exercised both in the real physical context and in the virtual one.

2. *The Communication on the definition of a European declaration on digital rights and principles: general aspects*

The Communication complements the proposed Declaration - which the Commission intends to sign solemnly and jointly with the European Parliament and the Council - setting out the digital rights and principles that should inform the activities of businesses, public administrations, policy-makers and individual citizens.

The two documents, as recalled, are only the last step (at least for the time being) of a path that the Union has been taking for some time in this field[6] and which, in its essential lines, is directed towards full respect for the fundamental rights of users in the digital environment, technological and net neutrality and inclusiveness, through the improvement of digital skills and competences.[7]

In particular, the common thread that binds the six chapters of the Declaration, but which, more generally, can be found in all legislation concerning the virtual environment, is the

[5] From the proclamation in Nice in 2000, to the *Laeken Declaration* of 2001, to the consecration in the *Lisbon Treaty* of 2009; in legal literature, for all, G. Tesauro, *Manuale di diritto dell'Unione europea*, edited by P. De Pasquale and F. Ferraro, III ed., Naples, Editoriale Scientifica, 2021, 151; A. Tizzano, *L'application de la Charte des droits fondamentaux dans les États membres à la lumière de son article 51, paragraphe 1*, in *Il diritto dell'Unione europea*, No. 3, 2014, 429; B. Nascimbene, *Carta dei diritti fondamentali, applicabilità e rapporti fra giudici: la necessità di una tutela integrata*, in *europeanpapers.eu*, Vol. 6, No. 1, 2021, 81.

[6] In addition to the 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final), see the Berlin Declaration on Digital Society and Value-based Digital Government, 8 December 2020, and the Lisbon Declaration – Digital Democracy with a Purpose, launched during the Leading the Digital Decade event on the 1 June 2021.

[7] As the *Communication* reads: "Between 12 May and 6 September 2021, the Commission carried out a public consultation to gather views on the formulation of European digital principles to promote and uphold EU values in the digital space. […] Overall, the consultations showed broad support for a European Declaration on Digital Rights and Principles as well as on the first set of principles outlined in the open public consultation, highlighting the importance of some of them over the others and with some respondents stressing the need for additional principles. The responses to the different consultation activities have guided the design of the Declaration presented today" (para 3).

need to ensure a fair, neutral and open online environment that respects the values on which the Union is founded. With this in mind, the Declaration places people at the centre of the digital transition, in addition to the values of the Union, and proposes a model that contributes to climate change and environmental protection.

The ambitious goal is governed by principles and rights that, while not yet formally defined, can be easily enucleated, given the level of detail of the "content" established and also in view of the fact that, in many Member States, "digital" regulation is at an advanced stage and can provide a valuable source to draw on.

Indeed, Article 6(3) TEU states that "the fundamental rights resulting from the constitutional traditions common to the Member States" are part of Union law, as general principles. These are, as is well known, principles that are proper to European Union law, to all intents and purposes and in their original form, even if they are the result of a mere recognition by the EU judge and do not find express enunciation in the Treaties.

In essence, the Declaration, which expressly states that it is based on the Union's primary law and, therefore, on the principles contemplated therein, represents in itself an expansive force for some of them and, at the same time, the formal container of the new generation principles, albeit - at the moment - broadly contemplated.

Among the classic principles destined to be shaped to the needs related to the digital transition, it is worth mentioning that of solidarity and inclusion, which should translate into the possibility of offering digital services to all, so that "no one is left behind".[8]

Closely linked to this principle is the one that envisages free participation in online democratic debate, considering the network's role in "orienting" public opinion and political confrontation.

Of particular relevance is then the principle of the sustainability of digital systems and devices, as there is now a widespread awareness that even information and digital technologies have an environmental impact.[9] The acceptance of this risk, in direct correlation with the shift in priorities, is well evident in the statement, which, in order to avoid significant damage to the environment and promote the circular economy, requires that digital products and services "should be designed, produced, used, disposed of and recycled in a way that minimises their negative environmental and social impact". And, adding that "everyone should have access to accurate, easy-to-understand information on the environmental impact and energy consumption of digital products and services, allowing them to make responsible choices".[10]

Among the so-called "new generation" principles, however, one should not forget the ethical ones that must inform the use of algorithms and artificial intelligence.

As is well known, the problem concerns above all the social policy sector because of the rapid spread of software and platforms used in a predictive function (release of benefits and performance), but also in a control function (verification and surveillance to prevent or sanction).

In fact, the risks of discrimination and violation of fundamental rights linked to the use of digital welfare state systems that make use of algorithms and big data are well known and can spread like wildfire to other sectors, since there are numerous projects that envisage the establishment of jurisdictional data sets and the creation of prediction models capable of representing the judge's reasoning.[11]

Precisely to address these dangers, the Declaration guarantees transparency and equality in the use of algorithms and artificial intelligence and prevents the predetermination of choices. And, consequently, states that "Everyone should be empowered to benefit

[8] On the topic, see G. Scotti, *Alla ricerca di un nuovo costituzionalismo globale e digitale: il principio di solidarietà "digitale"*, in *forumcostituzionale.it*, No. 2, 2021, 399.

[9] See *An SME Strategy for a sustainable and digital Europe*, 10 March 2020, COM/2020/103. For example, 1.7 tonnes of materials are used to manufacture a computer, including 240 kilos of fossil fuels; the internet alone consumes 10 per cent of the world's electricity and pollutes six times more than it did ten years ago, with emissions equalling international air traffic today; half an hour of streaming emits as much as ten kilometres travelled by car; mining a dollar of Bitcoin requires four times more energy than making one in copper and three times one in gold, etc.

[10] C. Gratorp, *The materiality of the cloud. On the hard conditions of soft digitization*, in *eurozine.com*, 24 September 2020.

[11] E.g., see the FRA report, European Union Agency for Fundamental Rights, *Getting the future right – Artificial intelligence and fundamental rights*, in *fra.europa.eu*, 14 December 2020.

from the advantages of artificial intelligence by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights".[12]

3. *The content of the digital rights envisaged by the Declaration*

Even with regard to the rights that must be respected throughout the Union, the Declaration draws a complex system that intersects traditional rights and new digital rights, many of them from the principles briefly examined.

It is necessary to reiterate that, in their "consolidated" scope, some rights are already guaranteed by the CFREU, and the interpreter, not without some difficulty, can limit himself to extrapolating them and adapting them to cases involving the use of digital technologies. On closer inspection, in fact, the primary objective of the Declaration, to ensure offline rights and freedoms also online, leads most situations in the digital world to the application of the principle of equality, read in conjunction with the relevant sectoral provisions.

The spread of digital systems has already revealed (and the trend is growing) special situations that do not find adequate forms of guarantee in the current regulation.

First of all, access to the digital system (internet) should be considered a true and proper autonomous right and, consequently, high-speed digital connectivity at affordable prices, everywhere and for everyone, should be protected by the competent authorities, thus properly implementing the principle of solidarity and inclusiveness. The right to access (or connection) should also be declined as a right preparatory to other rights, such as the right to education, the right to work, the right to information and freedom of expression.

Once again, the line between the present and the future becomes blurred, since some rights are already enshrined in the Charter of Fundamental Rights and are the subject of a granitic case law that ensures their broad protection; yet there is no doubt some that they must necessarily be "modernised".

Moreover, the right to disconnection should be expressly provided for, in close correlation with the social pillar referred to in the Communication and the proposed Declaration. Therefore, every EU citizen should be guaranteed adequate protection in the digital environment as well as in the physical workplace, irrespective of his or her employment status, mode or duration of activity.

Similarly, reference should be made to the rights of citizenship, starting with those to a protected digital identity, a digital domicile, to make electronic payments, to receive online public services, and to online transparency. Not forgetting, of course, the right to the security of one's own data, which, although the subject of a specific regulation, could not be left out of a Charter expressly dedicated to digital rights.

4. *Conclusions: horizons for a "digital constitutionalism" of the European Union*

The role that the Union is called upon to play in this area is unquestionably important. It is almost trivial to emphasise that, due to its supranational nature, it can intercept and protect the rights of the individual in cyberspace better than the Member States, where the absence of borders can become a determining factor for the acquisition of rights and freedoms, spontaneously allowing people to establish contacts beyond specific territories and offering new possibilities for learning and working beyond national borders.

With regard to this phenomenon, there has already been talk of "digital constitutional-ism", which, while representing a further and inevitable weakening of national sovereignty, could guarantee a single, high standard of protection through a harmonisation of digital rights in the European Union.[13]

Furthermore, a priority intervention by the Union, in the protection of digital rights, finds legitimacy in technical self-regulation which, if at the origin of the phenomenon justified and favoured the use of IT tools, then gradually turned into a boomerang with regard to the mechanisms put in place to safeguard virtual life, its contents and values.[14] That is, the digital world has led to a fragmentation of constituted power, which in some cases and in

[12] European Declaration, cit., Chapter III, para 9.

[13] For a general overview, G. De Gregorio, *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law*, vol. 19, No. 1, 2021, 41.

[14] M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in *La Rivista "Gruppo di Pisa"*, No. 2, 2021, 166.

some respects now belongs to private corporations (the digital platforms). The difficulty in tracing these patterns of power back to the classic vertical State-citizen relationship makes the protection of rights in the relevant legal situations more complicated (the citizen has no knowledge of how to protect himself, from whom to protect himself, who to protect himself against).

As has been observed, in a global digital environment, the risks to the Rule of Law principles do not come primarily from the ability of transnational private actors to develop and enforce private standards in competition with public values.[15]

The invisible but constant threat to its values has prompted the Union to emphasise several times in the proposed Declaration that they, like the rights of individuals, should be respected online as well as offline. Also from this perspective, an EU Charter of Digital Rights would be a useful tool to define the system of rights protection in a more sophisticated and up-to-date way, offering the Court of Justice a precise benchmark. In other words, it would enable the Court to respond to the demands for effective guarantees from the digital society, which will not fail to question it on issues that go far beyond the dynamics of the online economy and marketplace, as has been the case so far.

Finally, it should be noted that the "codification" of digital rights will follow a partially inverted process compared to the one that led to the Charter of Fundamental Rights, in that it will not be completely borrowed from the legal traditions of the Member States, but will also include rights that the Union itself will have "created" and then "cast" into individual legal systems. And, trying to be a bit visionary, it is hoped that, unlike the CFREU, the new Charter will be a uniform standard in the European legal space, irrespective of the shadow cone of the Treaties and the presence or absence of a situation of implementation of EU law. Also because, while discussing how to regulate these rights, cyberspace continues to evolve, creating virtual worlds in the digital world (the so-called metaverse). And people, through their avatars, live a real parallel life, in which we are already discussing how the related subjective rights, which we could call meta-digital, can be protected in the same way as in real life.

[15] O. Pollicino, *Costituzionalismo, privacy e neurodiritti*, in *medialaws.eu*, No. 2, 2021, 10.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 131-139
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 11

*Taxation and Tax Administration in the Digital Era – Polish Insigths**

Maria Supera-Markowska
(Doctor of Law, Assistant Professor, Department of Financial Law, Faculty of Law and Administration, University of Warsaw)

ABSTRACT Digitalisation is a trend we cannot fail to notice, both in social and economic relations. In the area of taxation, this brings about, in particular, the issue of inadequacy of existing solutions applied within specific substantive tax law to the digital economy. The following aspect of digitalisation in the area of taxation is the digitalisation of various types of formal and legal actions carried out by taxpayers in the fulfilment of their obligations. Finally, a third important issue is the use of digital tools and other opportunities offered by digitalisation for the tax administration to the execution of its tasks, including, above all, more effective tax control in a broad sense and the prevention of tax fraud. This article addresses these issues and their relationship, as well as some already existing solutions in the Polish tax system in this regard.

1. *Introduction*

Digitalisation is a trend we cannot fail to notice, both in social and economic relations. The growing significance of electronic communication, social media and online platforms, as well as the shift to remote working and learning, partly forced by the Covid-19 pandemic,[1] which, however, may be more permanent than originally anticipated, online banking and the development of cryptocurrencies through blockchain technology, e-commerce, e-services, e-government, e-health, etc. - these are all manifestations of the progressive digitalisation of the modern world, aspects of which could be enumerated further. In the area of taxation, this involves, in particular, the problem of inadequacy of existing solutions applied within specific substantive tax law to the digital economy (Spanish: *economía digital*, German: *Digitale Wirtschaft,* Polish: *gospodarka cyfrowa*), also known as the digitalised economy (Spanish: *economía digitalizada*, German: *Digitalisierte Wirtschaf*, Polish: *gospodarka scyfryzowana/cyfryzująca się*) and certain international projects designed to address these problems. The second aspect of the issue of digitalisation in the area of taxation is digitalisation of the various formal and legal actions carried out by taxpayers (as well as by tax remitters or other tax debtors) in connection with the fulfilment of their tax obligations (including, in particular, the submission of tax returns and other documents to the tax administration). Finally, a third important issue is the use of digital tools and other opportunities offered by digitalisation for the tax administration to the execution of its tasks, including, above all, more effective tax control in a broad sense and the prevention of tax fraud. This paper focuses on a presentation of the above-mentioned issues from the Polish perspective, using a dogmatic-legal approach and some empirical data. Poland ranks 24th of 27 EU Member States in the 2022 edition of the Digital Economy and Society Index (DESI) - however, between 2017 and 2022, Poland's aggregate DESI score grew slightly more than the EU average, signaling that Poland is catching up with the rest of the EU.[2] In this context it is especially worth mentioning that among the directions of operation and development of the Polish tax administration for the years 2021-2024, among others, the automation and digitalisation of its services and the digitalisation of the administration itself are indicated.[3]

* Article submitted to double-blind peer review.

[1] In fact, in case of tax administrations around the world they were already going digital and the pandemic has only accelerated the trend (cf. E. Constantin, *Tax administrations around the world were already going digital. The pandemic has only accelerated the trend*, in *Global Banking & Finance Review*, www.globalbankingandfinance.com/tax-administrations-around-the-world-were-already-going-digital-the-pandemic-has-only-accelerated-the-trend (access: 25 October 2022).

[2] European Commission, *Digital Economy and Society Index (DESI) 2022 Poland*, Brussels, 2022, 3, https://digital-strategy.ec.europa.eu/en/policies/countryes-digitisation-performance (access: 25 October 2022).

[3] Krajowa Administracja Skarbowa, *Kierunki działania i rozwoju Krajowej Administracji Skarbowej na lata 2021-2024*, Warszawa, 2020, www.gov.pl/web/kas/strategia-kas#:~:text=Czteroletnie%20kierunki%20dzia%C5%82ania%20i%20rozwoju%20Krajowej%20Administracji%20Skarbowej,pomiaru%20oraz%20zasady%20sk%

2. *Taxes and the digital economy*

2.1. *Inadequacy of existing taxation rules to the challenges of the digital economy*

The first of the tax problem areas related to digitalisation concerns the inadequacy of existing solutions applied within specific substantive tax law to the digital economy. The latter aspect is clearly visible in case of companies described as "digital businesses",[4] especially those operating internationally. The digital economy has changed the pattern of conducting a business activity and consumption in many ways, and existing business taxation rules cannot keep up with these developments.[5] These rules, in particular, are no longer suited to the current context, where not only cross-border trade but also the provision of services is possible without the physical presence of the entrepreneur in a given country. Hence, digital companies are active in a given national market often without a real presence there (as it is no longer necessary for them to sell their products there) but only through a virtual presence. As a result, under the current rules, taxable income cannot be assigned to the country of this market. In fact, these rules were developed for the traditional economy and the resulting right to tax income is assigned primarily on the basis of physical presence in a given country. Thus, a country in whose market a digital company operates virtually, often on a very large scale, may not have any rights to tax the profits of such a company if it is not resident or has a permanent establishment on its territory. However, even in case of a physical presence of the entrepreneur in a particular country allowing for taxation of the entrepreneur, the rules on the distribution of profits attributable to a permanent establishment may lead to the determination of a very low amount of taxable income in that country. In fact, the current tax rules do not take into account other specific characteristics of a digital business activity, such as in particular the significance of the users' contribution to value creation. Often, the main value for companies (called digital) is the content digitally generated by its users and the collection of data. This latter phenomenon is part of a wider issue - the new way in which value is being created within the digital economy and the lack of commensurability of taxation with the value so created.[6] This is a consequence of the fact that the traditional approach to measuring income for the purposes of its taxation is to determine the tax result on the basis of the revenues generated in transactions and the taxpayer's costs of earning them. Meanwhile, in the digital economy, the value created (e.g. user-generated digital content) is not always reflected in the form of revenue-cost transactions.

2.2. *Ad hoc solutions to problems - digital taxes*

The issues presented constitute a double challenge from a tax perspective. Firstly, the data acquired by the entrepreneur from users, which represent a significant element of value creation, may originate from a tax jurisdiction in which the digital entrepreneur does not have a physical presence, so the income from such activities is not taxable there. Secondly, even if the entrepreneur has a permanent establishment in the tax jurisdiction where the users are located, the value generated by the users is not taken into account in determining the taxable income there. In this context, the significant disparity in the real level of taxation of traditional and digital entrepreneurs is telling: the effective tax rate of the former is 23.2%, while that of the latter is 9.5%.[7] Such a situation creates distortions of competition (putting digital companies at

C5%82adania%20raport%C3%B3w%20z%20ich%20realizacji (access: 25 October 2022).

[4] See more: G. Kofler, G. Mayr and C. Schlager, *Taxation of the Digital Economy: A Pragmatic Approach to Short-Term Measures*, in *European Taxation*, No. 4, 2018, 126.

[5] R. Álamo Cerrillo, *La tributación de los servicios digitales. ¿Aplicación del principio de neutralidad o suficiencia?*, in M.Á. Collado Yurrita and L.M. Romero Flor (eds.), *Tributación de la economía digital*, Barcelona, Atelier, 2020, 177; G. Kofler, G. Mayr and C. Schlager, *Taxation of the Digital Economy: "Quick Fixes" or Long-Term Solution?*, in *European Taxation*, No. 12, 2017, 523; M. Olbert and C. Spengel, *International Taxation in the Digital Economy: Challenge Accepted?*, in *World Taxation Journal*, No. 1, 2017, 3; W. Schön, *Ten Questions about Why and How to Tax the Digitalized Economy*, München, Max Planck Institute for Tax Law and Public Finance, 2017, No. 11.

[6] M. Calabrese, *Taxation of the Digital Economy: A New Dawn for Multilateralism and Mutual Recognition*, in P. Pistone and D. Weber (eds.), *Taxing the Digital Economy. The EU Proposals and Other Insights*, Amsterdam, IBFD, 2019, 71.

[7] European Commission, Communication from the Commission to the European Parliament and the Council, *Time to establish a modern, fair and efficient taxation standard for the digital economy*, COM (2018) 146 final, Brussels, 2018, 4.

an advantage over other taxpayers) and thus violates the principle of tax fairness. Work has therefore been carried out both in the EU and within the OECD on a new concept of the taxation of entrepreneurs in a globalised digital economy. In the absence of tangible results in the expected timeframe, some countries (this has not been the case in Poland) have decided to introduce certain solutions in this regard unilaterally, adopting taxes defined as "digital",[8] in their tax systems, e.g. in Spain, introducing from 2021 a new tax on specified digital services (Spanish: *impuesto sobre determinados servicios digitales*, hereinafter referred to as IDSD).[9] The Spanish example cited here clearly illustrates how difficult it is to implement this tax[10] effectively: it was supposed to bring in EUR 968 million[11] to the state budget in 2021 which was only achieved to such a very limited extent that the planned revenue for the state budget from the IDSD in 2022 has already been set at the level of only EUR 225 million.[12] At the same time, according to the initial assumptions, this tax and other so-called digital taxes will lose their *raison d'être* once certain comprehensive solutions for the taxation of entrepreneurs are implemented as a result of the agreement at the OECD forum and the implementation of the BEFIT project in the EU.

2.3. *The OECD two-pillar agreement and the BEFIT project*

The agreement reached at the OECD forum in 2021[13] has two pillars. Pillar 1, discussions of which initially focused primarily on digital companies, aims to adapt international corporate profit tax rules to reflect the changing nature of business models, including taking into account the ability of companies to do business without a physical presence in a given country. Under it, countries will be given the right to tax a portion of the profits of certain non-resident companies by reallocating a portion of their global profits to jurisdictions where the company has customers or users, by applying an agreed formula. Pillar 2, on the other hand, is designed to reduce excessive tax competition between countries by ensuring a minimum level of taxation of multinational companies on all profits by supplementing the amount of tax paid by large multinational companies to a set minimum effective level. This minimum taxation of corporate profits is intended to reduce the potential for tax evasion. Effective coordination and cooperation in this regard will not be possible without ensuring the efficient operation of the tax administration, which in the current reality means, among other factors, a digitalised administration.

In the EU forum, actions both related to the OECD agreement and certain actions beyond it are set out in the *Business Taxation for the 21st Century*.[14] It indicates that the European

[8] See more: M. Supera-Markowska, *Podatek od usług cyfrowych – geneza, założenia i dalsze wyzwania*, in M. Bitner (ed.), *Problemy finansów i prawa finansowego. Księga jubileuszowa dedykowana profesor Elżbiecie Chojna-Duch*, Wrocław, Presscom, 2021, and the literature cited therein.

[9] M. Supera-Markowska, *Hiszpański podatek od usług cyfrowych – przyczynek do dalszej dyskusji o wyzwaniach podatkowych gospodarki cyfrowej*, in *Doradztwo Podatkowe. Biuletyn Instytutu Studiów Podatkowych*, No. 2, 2021, and the literature cited therein.

[10] Digital taxes, by their very nature, are burdened by a certain serious problem, namely that they require very specialised knowledge for, among other aspects, the application and control of the application of the tax rules, for which knowledge of many very technical issues and non-tax regulations is required, and the associated high administrative costs can undermine the fiscal efficiency of the tax (cf. M. Supera-Markowska, *Podatek od usług cyfrowych*, 307). This is in fact a broader issue than just related to digital taxes – digital transformation has generally made taxes multidisciplinary; their settlements and control in this area often require the involvement of specialists from IT departments, cooperating with accountancies, tax advisors or tax officials (cf. K. Feldo, *Ochrona praw podatnika w świetle technologicznej transformacji systemu* podatkowego, in *Doradztwo Podatkowe. Biuletyn Instytutu Studiów Podatkowych*, No. 4, 2022, 93).

[11] Ministerio de Hacienda y Función Pública, *Presupuestos Generales del Estado. Ejercicio presupuestario 2021*, Madrid, 2021, https://www.sepg.pap.hacienda.gob.es/Presup/PGE2021Ley/MaestroDocumentos/PGE-ROM/doc/1/2/1/2/1/N_21_E_R_2_101_1_2_198_1_101_1.PDF (access: 25 October 2022).

[12] Ministerio de Hacienda y Función Pública, *Presupuestos Generales del Estado. Ejercicio presupuestario 2022,* Madrid, 2021, https://www.sepg.pap.hacienda.gob.es/Presup/PGE2022Ley/MaestroDocumentos/PGE-ROM/doc/2/1/1/1/2/N_22_E_V_1_101_1_1_1_198_1_101_1.PDF (access: 25 October 2022).

[13] OECD/G20, Base Erosion and Profit Shifting Project, *Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy*, 2021, https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf (access: 25 October 2022).

[14] European Commission, Communication from the Commission to the European Parliament and the Council, *Business Taxation for the 21st Century*, COM (2021) 251 final, Brussels, 2021, hereinafter: COM

Commission is to propose a new framework for corporate taxation in Europe (the BEFIT project), which will be a single set of rules for corporate taxation in the EU based on two key features: a common tax base and the distribution of profits among Member States on the basis of a sharing formula (distribution), taking into account progress in global discussions, including those at the OECD forum. The BEFIT framework is designed to ensure, among other objectives, that entrepreneurs can do their business in the single market without unjustified tax barriers and, at the same time, to protect Member States against tax evasion.[15] It should not only contribute to the principle of fairness, but also to the principle of tax neutrality, and support the development of economic activity in the EU internal market by removing tax obstacles to such activity. Achieving these objectives requires a system of efficient and modern tax administration, hence the communication also draws attention to the need to digitalise it.[16]

3. *The organisation and tasks of the Polish tax administration*

Tax administration in Poland, comprising institutions and authorities dealing with the registration of taxpayers (and possibly other tax debtors), the assessment, control and enforcement of tax obligations and other tax-related issues, is organised primarily within the National Revenue (Tax) Administration (Polish: *Krajowa Administracja Skarbowa* - KAS). Its tasks, authorities and organisation are regulated by the provisions of the Act of 16 November 2016 on the National Revenue Administration (*ustawa z 16 listopada 2016 r. o Krajowej Administracji Skarbowej*) (UKAS).[17] Prior to the entry into force of the provisions of this Act, the tax administration (tax offices and tax chambers), the Customs Service (customs offices and customs chambers) and fiscal control (tax inspection offices) functioned independently of each other. At present, they all (after some changes) constitute a part of the National Revenue Administration, comprising tax offices, customs and tax offices and fiscal administration chambers.

The National Revenue Administration is a specialised government administration performing tasks in the field of the execution of, inter alia, tax revenues, as well as providing service and support to the taxpayers and tax remitters in the proper performance of their tax obligations as well as service and support to the entrepreneurs in the proper performance of their customs obligations (Article 1 (2) of the UKAS). The specific tasks of the KAS are set out in Article 2 (1) of the UKAS, according to which these tasks include i.a. the following:

- execution of revenues from taxes, fees and non-tax budget dues, as well as other dues, on the basis of separate regulations, with the exception of taxes and budget dues for which other authorities are competent;
- execution of revenues from customs duties and other charges related to the import and export of goods;
- providing service and support to taxpayers and tax remitters in the proper performance of their tax obligations and service and support to entrepreneurs in the proper performance of their customs obligations;
- execution of administrative enforcement of monetary claims and the provision of security for monetary claims;
- conducting information and education activities regarding tax and customs legislation;
- recognition, detection, prevention and combating of fiscal offences and fiscal misdemeanours and prosecution of their perpetrators.[18]

Pursuant to Article 11 (1) of the UKAS, the bodies of the KAS are: the minister competent for public finance, the Head of the National Revenue Administration, the Director of the National Tax Information, the directors of the fiscal administration chambers, heads of tax offices and heads of customs and tax offices. Under Article 13 of the Tax Ordinance Act[19] these bodies, according to their jurisdiction, are tax authorities. In addition to the KAS bodies, the role of tax authorities may also be fulfilled, as first instance bodies, by the relevant executive authorities of local

(2021) 251 final.

[15] COM (2021) 251 final, 11 ss.

[16] COM (2021) 251 final, 3 and 6.

[17] Uniform text: Journal of Laws of 2022, item 813 as amended.

[18] For more see e.g. A. Melezini, K. Teszner (eds.), *Krajowa Administracja Skarbowa: komentarz*, Warszawa, Wolters Kluwer, 2018 or L. Bielecki and A. Gorgol (eds.), *Ustawa o Krajowej Administracji Skarbowej: komentarz*, Warszawa, C.H. Beck, 2018.

[19] The Act of 29 August 1997 Tax Ordinance, *Ordynacja podatkowa*, uniform text: Journal of Laws of 2022, item 2651 as amended, hereinafter: Tax Ordinance Act.

government units (head of commune, mayor or city president) and by local government appeals colleges as appeal authorities.

4. *Digitalisation of tax settlements*

4.1. *Assessment of tax obligations and legal significance of tax returns in the Polish tax system*

As mentioned above, one of the basic tasks of the tax administration is the execution of tax revenues, which primarily involves the issue of assessment and collection of tax dues. In the Polish tax system, the assessment of taxes generally takes place within the framework of the so-called self-assessment - in accordance with Article 21(1)(1) of the Tax Ordinance Act, a tax obligation arises on the date of the occurrence of the event associated with the arising of such obligation under the tax act. In such a case, if the tax law requires the taxpayer to file a tax return, the tax presented in the tax return is the tax to be paid, and the date of payment is deemed to be the last day on which, in accordance with the provisions of the tax law, the payment should be made (Article 21(2) and Article 47(3) of the Tax Ordinance Act). Only in a few cases (e.g. real estate tax, agricultural and forestry tax for natural persons or inheritance and donation tax) does a tax obligation arise by way of an assessment made by the tax authority, i.e. on the date of delivery of the tax authority's decision setting the amount of that obligation (Article 21(1)(2) of the Tax Ordinance Act); in such a case, the tax payment deadline is 14 days from the date of delivery of the decision determining the amount of the tax obligation, unless the tax law provides for a later payment deadline (Article 47(1)-(2) of the Tax Ordinance Act).

4.2. *Provision of self-assessed tax returns to taxpayers by the tax administration on the tax portal*

A taxpayer obliged to self-assess his or her tax obligation in a tax return from 2019 onwards (for 2018) may use the declaration (return) prepared and made available by the tax administration through the tax portal ("Your e-pit" service"[20]). From the point of view of taxpayers who may benefit from this solution, it appears to be one of the most significant aspects of digitalisation of tax administration for them; however, it should be noted that the tax return availability service in question relates only to personal income tax settlements and only to those involving certain forms of taxation (using PIT-28, PIT-36, PIT-37 or PIT-38 forms); it is not applicable in particular to settlements relating to business activity, or to CIT taxpayers and other taxes.

The tax return made available on the tax portal within the framework of the "Your e-PIT" service is generated on the basis of data resulting mainly from information sent by tax remitters to the tax administration by the end of January concerning due advance payments on income obtained by the taxpayers in the previous tax year.[21] Pursuant to 45cd(1) of the Personal Income Tax Act (UPDOF),[22] as of 15 February of the year following a tax year, the tax authority shall make available to the taxpayer (with the exception of the taxpayer filing the tax return in connection with non-agricultural business activity or special divisions of agricultural production and the taxpayer being an inherited enterprise) tax returns via the tax portal, taking into account data held by the Head of the KAS, including data contained in the annual tax calculations and information from tax remitters, as well as data on advance payments made by the taxpayer during the tax year.

The taxpayer can accept the tax return - without or with changes, reject it or take no action on it. Acceptance by the taxpayer of the tax return before the expiry of the deadline for its submission, without or after making any changes to it, means submission of the tax return on the day of acceptance (art. 45cd(2) of the UPDOF); acceptance of the made available tax return is made by the taxpayer via the tax portal (art. 45cd(6) of UPDOF).

Where, prior to the expiry of the deadline for submission of the tax return, the taxpayer rejects (rejection is made by the taxpayer via the tax portal - Article 45cd(6) of the UPDOF) the tax return made available or fails to accept

[20] See: www.podatki.gov.pl/pit/twoj-e-pit (access: 25 October 2022). Currently, the 'Your e-PIT' service is available as part of the so-called e-Tax Office (www.podatki.gov.pl/e-urzad-skarbowy/?Polski-lad=true (access: 25 October 2022), which is intended to enable other matters than just those related to the annual tax return to be dealt with online. In fact, in addition to the "Your e-PIT" service, the system includes other functionalities, including, for example, a list of criminal fines or a tax micro-account number.

[21] In the Polish tax system, for PIT taxpayers, the tax year is the calendar year.

[22] Ustawa z 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, Personal Income Tax Act of 26 July 1991, uniform text: Journal of Laws of 2022, item 2647 as amended.

it, the taxpayer should submit the tax return in accordance with the rules set out in Article 45 of the UPDOF (except that in the case of a taxpayer who, in addition to income indicated in the annual tax assessment or information from tax remitters, has not obtained any other taxable income indicated in the tax return, failure to accept or reject the made available tax return before the expiry of the deadline for its submission means, pursuant to Art. 45cd(4) of the UPDOF, submission of the made available tax return on the last day of the deadline - automatic acceptance).[23] In such a situation, pursuant to Article 45cf(1) of the UPDOF, if the difference between the tax due and the sum of the advance payments due is not paid, the tax authority shall inform the taxpayer of the obligation to make the payment within one month from the date of expiry of the payment deadline, within 7 days from the date of delivery of this information. If the payment is made within 7 days of the date of service of this information, no interest on arrears shall be charged for the period from the day following the expiry of the deadline for payment of the difference (Article 45cf(2) of the UPDOF).

Article 45ce of the UPDOF contains regulations concerning the correction of the tax return made available on the portal in a situation where the submitted tax return contains errors or obvious mistakes resulting from a fault of the tax authority. In such a situation, the tax authority corrects the tax return, making the appropriate corrections or additions, and the taxpayer may file a possible objection to the changes (Article 45ce(1) of the UPDOF). Pursuant to Article 45ce(2) of UPDOF, no interest on arrears related to the adjustment shall be charged for the period from the day following the expiry of the deadline for payment of the tax until the expiry of the deadline for the taxpayer to raise an objection. Pursuant to Article 45cd(2a) of the UPDOF, if the taxpayer accepts changes made to the submitted tax return, this means submitting a correction to the tax return on the date of such acceptance. If this was the case when the taxpayer corrected the tax return in respect of errors or obvious mistakes caused by the authority before the correction was made by the tax authority, no default interest shall be charged on the arrears related to the correction of the tax return for the period from the day following the expiry of the tax payment deadline until the date of submission of the correction (Article 45ce(3) of the UPDOF).

4.3. *Automatic acceptance of made available tax returns and the risk of "tax illiteracy"*

As already indicated, the "Your E-pit" service is available from 2019 (for 2018). After the first two years of its operation, i.e. in 2021, the Ministry of Finance indicated that more than 10 million taxpayers (1 million more than the year before) had submitted their tax returns using this service for 2020, with this number including more than 4.3 million PIT-37 and PIT-38 returns automatically accepted.[24] It is therefore worth considering in this context to what extent the acceptance of the tax return prepared by the KAS is and should be a purely a formal act (or automatic at all), and to what extent it should indeed be a conscious verification merely of the proposal for settlement by the tax administration.

Automation has the undoubted advantage of simplicity; however, over a certain longer period, will it not lead to a kind of "tax illiteracy" among taxpayers, since they will not even have to read their tax returns? It is then possible that at some point they will become completely dependent on professional advisers or the tax authorities for their tax returns, the undesirable consequences of which in each variant of such a potential phenomenon probably do not need to be explained.... It is not only a problem of possible consultancy costs or consequences of overassessement of the tax obligation or underestimation of overpayment resulting from automated settlements (or, in particular, consequences for the third sector of automatic duplication of the National Court Register number when deciding on designation of a PIT deduction for a public benefit organisation), but rather the more general and potentially growing phenomenon of a lack of understanding of the nature of tax returns, aggravated by a lack of any real need to carry them out and likely to result in a growing lack of civic awareness of the assumptions, nature and actual implementation of the fiscal

[23] Unless the pension authority has made an annual tax assessment and the tax resulting from that assessment is the tax due under Article 34(9) or the taxpayer has filed the tax return without using the tax return made available by the tax authority (Article 45cd(5) of the UPDOF).

[24] www.podatki.gov.pl/pit/wyjasnieniapit/podsumowujemy-akcje-twoj-e-pit (access: 28 July 2022).

function and its relationship to the redistributive function of taxation.

5. *Digitalisation of taxpayers' reporting obligations*

5.1. *Uniform audit files*

The digitalisation of the tax administration not only concerns certain services for taxpayers, including in particular the provision of the tax return on the tax portal under the 'Your e-pit' service, but also the reporting obligations of taxpayers. At the same time, this issue mainly concerns entrepreneurs, where they are obliged to comply with the digitalisation requirements, including under the threat of certain penal and fiscal sanctions (meanwhile, in the case of the 'Your e-PIT' service, a special incentive to use it may be provided by the regulation contained in Article 77(1)(5a) of the Tax Ordinance Act, according to which an overpayment resulting from the tax return submitted by means of electronic communication is subject to refund within 45 days - and not the standard 3 months - from the date of submission). Thus, we are talking about the "forced" (compulsory) digitalisation of taxpayers, however, at least to a certain extent, e.g. electronic submission of tax returns, accepted as a convenience rather than an onerous obligation. It is worth starting with the most fiscally important tax in the Polish tax system, namely value added tax (VAT)[25] and the uniform audit files, for a certain characterisation of the obligations in this respect.

The Uniform Audit Files (Polish: *Jednolity Plik Kontrolny* – JPK) are the equivalent of the Standard Audit File for Tax (SAF-T). They are now mandatory to be submitted electronically in a form integrated with the VAT return. By providing purchase and sales data in this way, they are expected to significantly improve the work of the tax authorities, who can quickly carry out checks and controls. Access to structured data is intended to enable the tax administration to identify irregularities in an expeditious manner, enabling it in particular to counter such phenomena as VAT fraud or tax evasion, and to speed up the confirmation of correct accounts in the case of honest taxpayers. Thanks to the shortening of the period of checking and control activities, and thus the reduction of the related costs, both administrative - on the part of the tax authorities - and compliance costs - on the part of the taxpayers, not only the tax administration but also the taxpayers should benefit from the introduction of the Uniform Audit Files (JPK). This trend in the digitalisation of the tax administration, i.e. the digital provision of data to the tax administration for extensive tax settlements verifications, can also be observed in the area of other taxes.

5.2. *Electronic submitting of tax returns and financial statements*

Currently, the obligation to submit tax returns electronically also applies to returns for taxes other than just VAT; in particular, the tax returns of corporate income tax taxpayers. In case of income taxes, we should also mention the electronic transmission of financial statements to the tax administration. Under the current legal status, entities entered into the Register of Entrepreneurs in the National Court Register (Polish: *Krajowy Rejestr Sądowy* - KRS), in accordance with Article 69(1) of the Accounting Act,[26] should file the approved annual financial statements (together with certain other documents) with the competent court register, i.e. the National Court Register, within 15 days from the date of approval. If the statement has not been approved within 6 months of the balance sheet date, it shall be submitted within 15 days thereafter, and then also within 15 days after its approval, together with the relevant documents (Article 69(2) of the Accounting Act.). These rules apply *mutatis mutandis* to the parent company preparing the annual consolidated financial statements of the group (Article 69(3) of the Accounting Act). The statements, which are prepared electronically and in an appropriate structure or format, must be transmitted by means of electronic communication.[27] These entities are now no longer obliged to additionally self-report their financial statements to the tax administration (since they submit them electronically to the National Court Register). On the other hand, entities not listed in the Register of

[25] VAT accounts for almost half of the revenue of the state budget; and among its tax revenues - over 50% (see state budgets: www.gov.pl/web/finanse/ustawy-budzetowe).

[26] Ustawa z 29 września 1994 r. o rachunkowości, Accounting Act of 29 September 1994, uniform text: Journal of Laws of 2023 item 120 as amended, hereinafter Accounting Act.

[27] See: https://e-sprawozdania.mf.gov.pl/ap/#/step2-start (access: 25 October 2022).

Entrepreneurs in the National Court Register should submit their financial statements (possibly together with certain other documents) to the Head of the National Revenue Administration:

- corporate income taxpayers within 15 days from the date of approval of the annual financial statements (Article 27 (2) of the Corporate Income Tax Act[28]);
- taxpayers of personal income tax before the deadline set for the submission of the tax return, i.e. 30 April of the year following the tax year (Article 45 (5) in conjunction with item 1 of the UPDOF).

Pursuant to Article 80b of the Fiscal Penal Code[29] whoever, contrary to his/her obligation, fails to submit a financial statement or an audit report to the competent tax authority on time, shall be liable to a fine for a fiscal offence. The submitted financial statements are made available by the Head of the National Revenue Administration to the heads of tax offices, heads of customs and fiscal offices, directors of tax administration chambers and the minister in charge of public finance (Article 27(2b) of the UPDOP and Article 45(8a) of the UPDOF).

At present, however, the equivalent of the Uniform Audit Files (JPK) in income taxes has not yet been implemented in Poland. Although the so-called "Polish Deal" (Polski Ład)[30] stipulated that, as of 2023, entities maintaining accounting and other tax books would be obliged to maintain them using computer programmes and send them to tax offices by means of electronic communication in an appropriate electronic form, the effective date of the obligations in this respect was postponed in 2022[31] (until accounting periods beginning after 31 December 2023, after 31 December 2024 or even only after 31 December 2025 - depending on the category of taxpayers).

5.3. *Analysis of reporting data by the tax administration*

In the context of taxpayers' reporting data transmitted electronically to the tax administration, a fundamental issue concerns ensuring that this data is subject to appropriate analytical processes. Digitalization of the taxes should be treated only as an instrument for achieving the goals of tax system, not to be an end in itself.[32] In this context, it is worth noting that while the harmonised VAT system does not pose any major specific challenges for the Polish tax system in this respect, it should be noted that under Polish income tax regulations, as a rule, the tax result and the financial result are determined independently of each other: for tax purposes in accordance with the provisions of the income tax acts, while for financial accounting purposes on the basis of the relevant regulations of the balance sheet law and financial reporting standards.[33] There are numerous differences between the two areas (resulting in both temporary and permanent differences between tax and financial results). The analysis of financial statements for tax purposes is therefore not straightforward. Meanwhile, any arrangements for the submission of data by taxpayers to the tax administration must be assessed through the prism of the possibility and appropriateness of analysing them and a reasonable relationship of proportionality between the means used and the objectives to be achieved should be maintained.[34] This also applies to other instruments and solutions within the framework of the digitalised tax administration, including in particular the obligation for beneficiaries and other persons involved in their design and implementation to disclose tax schemes (Mandatory Disclosure Rules[35]), the ICT system of the clearing house

[28] Ustawa z 15 lutego 1992 r. o podatku dochodowym od osób prawnych, Corporate Income Tax Act of 15 February 1992, uniform text: Journal of Laws of 2022, item 2587 as amended, hereinafter UPDOP.

[29] Ustawa z 10 września 1999 r. Kodeks karny skarbowy, Act of 10 September 1999. Fiscal Penal Code, uniform text: Journal of Laws of 2023, item 654.

[30] Introduced by the Ustawa z 29 października 2021 r. o zmianie ustawy o podatku dochodowym od osób fizycznych, ustawy o podatku dochodowym od osób prawnych oraz niektórych innych ustaw, Act of 29 October 2021 amending the Personal Income Tax Act, the Corporate Income Tax Act and certain other acts, Journal of Laws item 2105 as amended.

[31] By the Ustawa z 9 czerwca 2022 r. o zmianie ustawy o podatku dochodowym od osób fizycznych oraz niektórych innych ustaw, Act of 9 June 2022 amending the Personal Income Tax Act and certain other acts, Journal of Laws item 1265 as amended.

[32] Cf. K. Feldo, *Ochrona praw podatnika w świetle technologicznej transformacji systemu* podatkowego, in *Doradztwo Podatkowe. Biuletyn Instytutu Studiów Podatkowych*, No. 4, 2022, 95.

[33] See more.: M. Supera-Markowska, *Rachunkowość - aspekty prawne i podatkowe*, Warszawa, Wolters Kluwer, 2022.

[34] For more see A. Mudrecki, *Zasada proporcjonalności w prawie podatkowym*, Warszawa, Wolters Kluwer, 2020.

[35] See more: Krajowa Administracja Skarbowa, *Sprawozdanie Szefa Krajowej Administracji Skarbowej w zakresie informacji o schematach podatkowych*

(STIR)[36] or electronic list of VAT taxpayers (the so-called white list of taxpayers).[37]

6. *Conclusions*

The issues of digitalisation in the tax area are related to the problem of the inadequacy of the existing solutions of substantive tax specific law to the challenges of the digital economy and the formal and legal actions carried out by taxpayers (tax remitters or other tax debtors) in connection with the fulfilment of their tax obligations, as well as the use of digital tools and other opportunities created by digitalisation by the tax administration for the performance of its tasks, including, above all, more effective tax control in a broad sense. In the former context, certain solutions developed on an *ad hoc* basis in the form of so-called digital taxes will lose their *raison d'être* once comprehensive changes to business taxation are implemented as a result of the two-pillar agreement at the OECD forum and the implementation of the BEFIT project in the EU. However, for their effective implementation, it will be necessary, among other aspects, to ensure the smooth functioning of a modern tax administration, which in the current reality means, inter alia, its digitalisation. This digitalisation refers to the implementation of certain solutions for taxpayers (and other tax debtors) to facilitate the fulfilment of their tax obligations, such as, in particular, making tax returns available on the tax portal for taxpayers, which in Poland operates under the "Your e-PIT" service. It also manifests itself in the imposition of electronic reporting obligations on tax debtors, such as the Uniform Audit Files (JPK) or e-financial statements.

In general, it can be concluded that some of the facilitations resulting from the digitalisation of administration in the Polish tax system, are directed only to taxpayers who are not engaged in economic activity, while certain tax incentives are provided for the use of these solutions (faster timeframe for refunding overpayments). In contrast, for entrepreneurs, even if there are certain facilitations, at the same time many obligations are imposed on them (e.g. with regard to JPK, e-financial statements or the future obligation to submit electronic tax books to the tax administration). This is linked to another aspect of the digitalisation of tax administration, namely the obligations imposed on tax debtors to digitally transmit tax-relevant data to the administration, which, through their ongoing analysis, is expected to have an increased ability to prevent tax fraud events. It is crucial in this context that this data are genuinely and continuously analysed and that appropriate conclusions are drawn from them, and that the very process of introducing new obligations on taxpayers is properly carried out (with an appropriate *vacatio legis*, in a transparent and comprehensible manner). It is important to note that the costs of complying with the requirements of digitalised data transfer (rather than options - as in the case of non-professional entities) are borne not only by the tax administration, but also by entrepreneurs. These costs can be justified if, through the identification of irregularities, a fairer tax system is implemented, which - ultimately - should benefit all taxpayers and society as a whole.

In the long perspective, the increasing use and development of digital technologies will lead to a further redefinition of the world of taxation and its settlement, with possible risks associated with this (including in particular insufficient processing of data collected or "tax illiteracy") but also opportunities, among which the primary benefit is expected to be the implementation of a fair tax system and the elimination of barriers to the development of economic activities. In doing so, the related issues should be considered comprehensively, taking into account both the principles of determining the tax burden itself and the distribution of the tax revenues derived therefrom, as well as the formal and legal obligations of taxpayers and the analytical and control activities of the tax administration itself.

przekazanych w latach 2019-2021, Warszawa, 2021, www.gov.pl/web/kas/struktury-mdr (access: 25 October 2022).

[36] See more: Ministerstwo Finansów, Krajowa Administracja Skarbowa, *Sprawozdanie w zakresie przeciwdziałania wykorzystywaniu działalności banków i spółdzielczych kas oszczędnościowo-kredytowych do celów mających związek z wyłudzeniami skarbowymi za 2020 rok*, Warszaw, 2021, www.gov.pl/web/kas/struktury-stir (access: 25 October 2022).

[37] See: www.podatki.gov.pl/wykaz-podatnikow-vat-wyszukiwarka (access: 25 October 2022).

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 141-149
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 12

Artificial Intelligence, Tax Law and (Intelligent?) Tax Administration

Luís Manuel Pica

(PhD in Public Law at University of Minho (Portugal). Assistant Professor at Polytechnic Institute of Beja (Portugal); Researcher at JusGov- Research Centre for Justice and Governance at University of Minho – School of Law (Portugal))

ABSTRACT Artificial intelligence has entered our lives to change paradigms, create new methods for agents to act and allow the evolution of human interests. Its application by the tax administration is also an inevitability, allowing a better administration, a closer relationship with the taxpayer and a better management of the tax system. But the strong palpitations and the existing heterogeneity of application are issues that cannot fail to be analysed.

1. *Introduction*

The intersection of artificial intelligence with common, everyday life is today an undeniable reality. Think about the simple purchase of a piece of clothing on the internet, the consultation of news that we do on our smartphone, or the mere playback of music. Through the collection of personal data and the digital footprint left by these (and other acts) artificial intelligence and the mass processing of personal data can create an accurate profile about our tastes, lifestyles, and our own daily lives.

Man's ancestral yearning for perfection and his desire to control everything around him is today a truth that is not insignificant, and the application of artificial intelligence in the various relationships established by man is irrefutable proof of this desire. The search for perfection has led man to adopt systems of mechanisation of his own acts, namely through the automation of processes and procedures. Through the artificial replication of man's manual capacity, technological systems can perform the acts, conduct and actions included in each procedure, following mathematical and syllogistic models programmed sequentially in a computer programme, replacing the human function. But this "intelligence" goes further and can be classified as true "thinking machines", which are attributed the ability to imitate human thought, its cognitive reasoning and learning new formulas that can later be used to solve new problems.

However, the sectoral integration of systems capable of automating procedures and imitating human thinking has been varied. The e-commerce and economic sectors have been priority areas in the application of these systems. But we cannot fail to mention that their importance is also growing in Public Administration itself. A good administration, close to the citizens and providing a good public service, is a requirement of contemporary States. Through the application of automated and artificially "intelligent" systems, it will be possible to achieve maximum efficiency and effectiveness, as well as savings in the costs inherent to administrative management. The administrative modernization cannot but be a constant, but we cannot fail to mention that its field of action does not bring something new. Therefore, artificial intelligence can (and should) be used to support the administration in the fulfilment of its tasks.

2. *Terminological clarifications on artificial intelligence*

A serious study of the theme involves concepts, qualifications, categories, and types that go far beyond the purposes of this paper.

Considering that artificial intelligence assumes different stages, classifications, or intensities, we can (and should) make a brief contextualization that allows us, in accordance with the degree and capacity of autonomous problem solving and its autonomy in relation to man, to delimit the concepts of artificial intelligence, from analogous and close concepts, but which are often used indistinctively.

In this sense, we can find an artificial intelligence of variable intensity, that is, whose classification can be made by

* Article submitted to double-blind peer review.

consideration of its ability to imitate man.[1] Thus, we can find a strict, strong artificial intelligence or superintelligence *(schwacher und starker Künstlicher Intelligenz*). According to this contextualisation, a strict artificial intelligence focuses on solving concrete application problems based on purely mathematical methods, replicating what is previously ordered by man. On the contrary, the strongest expression of artificial intelligence is supposedly configured with the ability to imitate man and his deductive and cognitive power.[2] If the latter is overcome, the result is a superintelligence, capable of surpassing the human being itself.

The classification into narrow artificial intelligence, strong artificial intelligence and artificial superintelligence has the same concrete objective, but distinguishable in one of administrative applicability. In narrow artificial intelligence, systems are developed for specific problems, whose solution usually requires a certain scope and a certain form of intelligence. A characteristic example is the verification of tax declarations, or mechanical application of previously programmed acts, whose contours do not show much discretionary or evaluative capacity. Intelligence artificial *strong and artificial superintelligence* pursue, in turn, the goal of building a system that has an intelligence comparable or superior to that of a human being.

This leads us to state that artificial intelligence, when applied to Law, is here understood as the non-human (machinal) aptitude to generate a probabilistic meaning to which certain legal effects are imputed. Therefore, when we speak of artificial intelligence applied to Tax Law, we speak, essentially, of a non-human aptitude, capable of foreseeing and anticipating conducts, of performing acts in a mechanized manner and to which legal-tax effects are attributed, constituting, or modifying the taxpayers' legal sphere. It is from this applicability and interference in the legal sphere of the subjects that the Law will have to give shelter to the acts and conducts practiced by artificial intelligence. The intervention of Law will be necessary and unmistakably imperative when the acts of thinking machines interfere with the legally protected rights and interests of subjects.

However, we cannot fail to delimit concepts that are similar but cannot be confused. In systematic terms, the German doctrine[3] has been proliferating in this study, so we have drawn on his studies to refer to the following conceptual delimitations and terminological clarifications:

- "Artificial intelligence" (*Künstliche Intelligenz*): refers to the attempt to reproduce understanding and learning through an artefact, focusing mainly on thought and action, and aiming at a rational ideal or a replication of human capabilities.
- The "artificial intelligence technology" (*Künstliche Intelligenz Technologie*): refers to individual functions that can be implemented in computers to achieve certain goals, using artificial intelligence techniques (e.g. machine learning).
- The "artificial intelligence system" (*Künstliche Intelligenz System*): means a structured and contextualised combination of various artificial intelligence technologies, with the aim of achieving conclusions and results like those achieved by humans, but in a mechanised way.
- "Artificial intelligence decisions" (*Künstliche Intelligenz Entscheidungen*): are conclusions of artificial intelligence systems with real-world implications that depend on human decisions at the system design level, the strategic level (deciding how to use the system) and the tactical level (shaping the interaction with the person using the system).

Considering that the function of Law is not to regulate concepts, nor to refer to terminological notions, it is up to the academia and experts in the field to provide the necessary contribution for us to accurately understand the varied technological realities that are employed by society. Not understanding this would lead us into dangerous fields that we cannot avoid, falling

[1] In this sense, see the distinctions between "weak" (schwache KI, artificial narrow intelligence), "strong" (starke KI, artificial general intelligence), or "super strong" (Superintelligenz, artificial superintelligence) artificial intelligence. A. Bleckat, *Anwendbarkeit der Datenschutzgrundverordnung auf künstliche Intelligenz*, in *Datenschutz und Datensicherheit*, vol. 44, No. 3, 2020, 195.

[2] C. Würschinger, *Künstliche Intelligenz – Zwischen Wunsch und Wirklichkeit*, in *Wirtschaftsinformatik & Management*, 2020, 86.

[3] C. Schmidt, *The Future Use of Artificial Intelligence in the German Tax Administration - Decision Support in the Context of Hybrid Case Processing*, in *EasyChair Preprint*, No. 7644, 2022, 4.

into a terminological redundancy that leads us in a conceptually erroneous direction.

3. *Artificial intelligence, tax procedure and procedural automation*

Focusing our speech on the integration of artificial intelligence in the scope of the tax procedure and process, it is assumed, first, that this analysis must include a clear notion of what we should understand by "tax procedure". Only when this concept is assumed, can we make an analysis of the integration of artificial intelligence in it.

Using the teachings of Joaquim Freitas Da Rocha,[4] the classic tax procedure is based on a set of acts, from distinct legal-tax actors, relatively autonomous and sequentially organized, directed to the production of a certain result, of which they are instrumental. By way of this notion, we refer that these volitional statements issued by administrative bodies with legitimacy for such, may be left to artificial intelligence systems, so that they may perform these tasks, according to mathematical and programmatic models delimited in the algorithm used by the computer system.[5]

It is understandable that this same procedure cannot escape the impulses of a post-modern society. The impulses of a society based on information and communication technologies - reaching futuristic contours - brings with it the need to reformulate the support used in the procedures carried out by the tax administration, making them dematerialized and automated. Considering only the actions of the tax administration, it is enough to think, for instance, of notifications or summonses being served electronically, obliging some taxpayers to have an electronic domicile; of the automatic offsetting of tax credits and debits regarding a certain taxpayer; of the submission of electronic declarations, previously filled in and semiautomatic; of the commencement and processing of a tax enforcement procedure; of the electronic attachment order of pecuniary amounts to banks; or even of the electronic auction in the sale phase of a tax enforcement procedure. In all these cases, the physical materiality of the acts performed is waived, preferably emanating in the form of digitalised acts, and the biological will be directly waived, giving precedence to the practice of automatic acts.[6] [7]

However, and considering the terminological universe previously assumed, it cannot be said that the application of artificial intelligence in the context of tax management is achieved in a uniform way. This understanding leads us to differentiate artificial intelligence applied to tax management in two different ways: (i) procedural automation; (ii) artificially intelligent action of the administration; and (iii) artificially intelligent performance of the administration.[8]

[4] J.M. Freitas Da Rocha, *Lições de Procedimento e Processo Tributário*, IV ed., Coimbra, Coimbra Editora, 2011, 83.

[5] "The algorithm, in general terms, can be defined as a process, a sequence of operations that allow to solve a problem in a finite number of steps, in compliance with two requirements: i) each step of the sequence must already predefine the next step and ii) the result to which the sequence tends to must be concrete, real, useful". A. Coiante, *The Automation of the Decision-making Process of the Public Administration in the Light of the Recent Opinion by the Italian Council of State Regarding the Draft of Regulations Concerning the Modalities of Digitalization in the Public Tender Procedures*, in *European Review of Digital Administration & Law*, vol. 2, No. 1, 2021, 239; L.M. Pica, *El uso de la Inteligencia Artificial por parte de las Administraciones Tributarias: ¿Una Necesidad o una Utopía?*, in F. Serrano Antòn (ed.), *Inteligencia Artificial y Administración Tributaria: Eficiencia Administrativa y Defensa de los Derechos de los Contribuyentes*, Navarra, Thomson Reuteurs, 2021, 532; G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Naples, Editoriale Scientifica, 2019, 5.

[6] It should be noted that, in all these cases, this artificially intelligent system does not have a natural or resultant will, but merely follows a predetermined sequence and externalizes a result, denoting an automated will without the possibility of choice, in view of the data inserted and the sequencing of previous actions. It is still possible to reconstitute the entire procedure and in it a human will can be glimpsed, albeit somewhat receded and accompanied by automatisms which, without transcending it, replace it operationally. Hence affirming that the purely biological will is dispensed with, but in an apparent way, since human action ends up being effectively materialized through the programming of the algorithm used by the artificial intelligence system. V. Pereira Da Silva states that "[é] o comportamento humano que condiciona e determina as operações automatizadas, pelo que, em última análise, a responsabilidade pelas decisões processadas por intermédio de computador é de imputar a indivíduos, e não a uma qualquer máquina". V. Pereira Da Silva, *Em busca do Ato Administrativo Perdido,* Coimbra*,* Almedina, 1998, 483 ss.

[7] J. López Camps, A. Gadea Carrera, *Una nueva Administración pública. Estrategias y métodos para mejorar la calidad y la eficiencia del e-Gobierno*, in *Instituto Vasco de Administración Pública*, 2001, 23.

[8] C. Schmidt, *The Future Use of Artificial Intelligence in the German Tax Administration - Decision Support in*

When we talk about a (i) procedural automation, we cannot fail to mention the notion of classic procedure that underlies the understanding of the doctrine. The notion of procedural automation cannot but be based on this premise, consisting of the practice of a set of acts, sequentially organised and previously programmed by man and materialised in a computer algorithm, which will be used by a computerised system that, because of the input data, will determine the practice of a tax administrative act. Inevitably, the following are essential requirements for procedural automation: the existence of an algorithm which informatically materialises the legal-procedural rules; a computer system which will apply the algorithm, collecting and reading personal input data; finally, in accordance with the input data and the sequence predetermined in the algorithm, the acts will be performed in a fully automated manner and with little human intervention.[9] We essentially speak of a strict or inappropriate artificial intelligence because the technologies are not so innovative, and their use is criticised. The automation of decisions is suggested as a preferable term.

On the contrary, the (ii) performance of an artificially intelligent administration develops through the integration of artificially intelligent systems, which will replace the human capacity of the agents and employees who integrate the administration and will lead to a purely mechanical activity of the administrative procedural activity. We speak, thus, of the replacement of the human capacity of the administration by a mechanical capacity capable of replacing man and his activity in the tax procedure.[10]

The tax administration cannot neglect its task of collecting tax revenue and cannot be held hostage to the dogmatic ties that underlie the classic performance of administrations. It is unquestionable that new techniques, new tools, and new horizons are needed to respond to the needs of a globalised and open society. The public administration itself (and inherently the tax administration) is not immune to the evolution of new social demands. Therefore, the procedural automation, the integration of intelligent systems and the modification of the relationships established between the administration and the subjects must be rethought. It is up to the tax administration to know how to use them and how to make the best use of them. It will be by using machines capable of emulating human cognitive processing that it will be possible to achieve new ratios of efficiency and increased results to meet the constitutional requirements to which the State itself is bound.

4. *Artificial intelligence in tax management*

Trying to locate the concrete applicability of artificial intelligence with reference to the considerations above, it is easy to see that an artificially "intelligent" tax procedure is one that seeks to support its decision-making acts in automatic schemes and support the activity of agents and officials who make up the administration. The conception of an activity supported by intelligent systems allows its integration according to a double dimension: i) a purely external dimension, in which the activities performed by intelligent support systems are visible to taxpayers; ii) an internal dimension, through which, the acts performed and the internal and routine activities - which are the core of the tax administration's activity - are not so visible to taxpayers.

On the other hand, the possibility of collecting and processing personal data and information at an incredibly fast pace ends up allowing a supervision and control over taxpayers' acts, also allowing the creation of risk patterns (profiles) that lead to conclusions, for a future action of the administration.[11]

Let us look at each of them in detail.

the Context of Hybrid Case Processing, 4.

[9] We cannot fail to mention that in order to carry out these acts, the following must be achieved beforehand: the programming of the system through the pre-sequencing of legally foreseen stages, which translates into what the legal doctrine calls the "computerisation of legal rules"; the insertion of data and input information; and the access of legally qualified individuals, through registration and authentication, all taking place in a network, in a mechanical and automatic environment.

[10] L.M. Pica, *El uso de la Inteligencia Artificial por parte de las Administraciones Tributarias: ¿Una Necesidad o una Utopía?,* 532.

[11] L.M. Pica, *The new challenges of artificial intelligence, profiling and bigdata analysis by tax administrations: will the right to meet these new challenges be shown?,* in *Top 10 Challenges of Big Data*, Nova Editora, 87; L. Scarcella, *Tax compliance and privacy rights in profiling and automated decision making*, in *Internet Policy Review*, vol. 8, No. 4, 2019, 1; S. Stefanelli, *Diritto e Intelligenza artificiale. Alcune riflessioni nell'ambito del paradigma argomentativo*, in *Informatica e diritto*, vol.VIII, No. 1, 1999.

4.1. *The applicability of artificial intelligence in front-office and back-office activities*

The discursive anchoring should now be directed to the concrete application of artificial intelligence in tax management. In this sense, we cannot fail to mention that the activity of artificial intelligence requires a huge amount of information, which is essential for the full operation of an artificially intelligent administration. We are talking about a large volume of personal data of (and about) taxpayers, without which the use of artificial intelligence systems (either strictly or super strong) is inoperable and without functional content that allows compliance with the requested requirements.

Public administration in general - and financial administration in particular - has such personal data, through various sources. Due to the large amount of data that is collected annually through the procedures of mass collection of personal data, together with the typically established and largely standardized and structured processes in the various legal systems, this administrative area is predestined for the use of artificial intelligence.[12]

However, a useful differentiation could lead us to its application in (i) socially external activities (front-office) and (ii) socially internal activities (back-office).[13] Within both, we can find as primary activities of use of artificial intelligence, the application of intelligent systems through decision support measures and/or through instruments aimed at the automation of the procedure itself and administrative decision-making:

1) When we talk about socially external activities (front-office), we refer to the fact that artificial intelligence systems can serve as support in receiving and supporting taxpayers. In other words, the focus is on contact with taxpayers and, the greater the guidance given by artificial intelligence in supporting taxpayers' questions and doubts, the stronger will be the access to good administration and the achievement of this desideratum, since taxpayers will be easily corresponded to their needs and expectations.[14] We are talking, therefore, about a digital access in which the thinking machine is conceived, predominantly, as a source of information and support for taxpayers. The use of artificial intelligence by the administration thus opens completely new possibilities for taxpayers' contact with the administration to be simple and uncomplicated, uncomplicating relations and earning taxpayers the most pleasant attention possible.
2) On the contrary, the use of artificial intelligence for socially internal sectors (back-office), appears as a more reserved measure and of application to support and back up the agents and officials of the administration. The application of intelligent systems by the tax administration seeks support and massive collection of personal data, as well as support for internal processes. It is one of the most important uses by the tax administration, as internal processes are becoming more and more important as administrative structures, economic relations and relations between society become more complex.

In both situations presented, the use of artificial intelligence in the context of tax management, the support processes do not generate the creation of value, but they allow and/or promote that the procedures are profitable, according to a greater criterion of efficiency.[15] Considering that the

[12] Such personal data may be collected through several modalities. We may refer to the classic collection of personal data, namely through the information procedures available to the administration and enshrined by the legislator since the beginning of the so-called "privatisation" of the tax management system (e.g. tax inspection procedures, declarations of taxpayers and third parties, etc.); but, we may also refer to the innovative models of tax information collection, namely through social network profiles and the creation of profiles and cataloguing of activities or third parties.); but we can also mention the innovative models for collecting tax information, particularly through social network profiles, the creation of profiles and cataloguing of risk activities or subjects, or even through the widespread automatic exchange of information between states, with the collaboration of taxpayers and third parties.

[13] C. Schmidt, *The Future Use of Artificial Intelligence in the German Tax Administration - Decision Support in the Context of Hybrid Case Processing*, 6.

[14] European Commission, Plano Coordenado para a Inteligência Artificial, Com (2018), 795 final, Brussels, 7 December 2018, 21, avaliable at https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM:2018:795:FIN.

[15] "La transformación digital se entiende como la integración de nuevas tecnologías en las entidades para cambiar su forma de funcionar. Es claro que el trasfondo de este concepto corresponde a acciones que llevan a optimizar procesos en el que se requieren menos recursos para lograr excelentes resultados. También en mejorar la productividad donde buscamos

administration's resources are limited, the aim is to make the most of them, to make the most of them.

Therefore, it is of great interest to simplify procedures, namely through their automation. The objective of using artificial intelligence is, therefore, to relieve human resources from assistance activities and administration support processes. The aim is for support procedures to be carried out by machines, as they achieve a more prolific result and, as a counterpart, a better result in available human capacities, as they are reallocated to sectors or activities where they can perform suitable and less tedious and bureaucratic tasks.

Furthermore, the procedural decisions that derive from an analysis by mechanical systems can be classified as more effective, more objective, and less susceptible to being syndicated based on subjectivism or human error. The evaluation of the data and information that are framed by the corresponding tax legislation is more efficient and effective if done by intelligent systems. First and foremost, we are talking about the fact that man can be assisted in making the corresponding decision, with the machine in this situation "advising" on the correct decision-making according to the data and information provided (e.g. providing recommendations on the course of the procedure and on any (discretionary) room for manoeuvre that can be directly taken into account in the decision-making process).

In a more utopian perspective, the agents and officials legally entitled to take the corresponding decisions, as well as the agents and officials in charge of the instruction of the tax procedure/proceedings, may be completely replaced using artificial intelligence. During full automation, the human being is completely removed from the decision-making procedure/process and binding decisions are taken autonomously by entities endowed with artificial intelligence. Human resources are thus freed from monotonous work (perceived as irritating and tedious), leaving these tasks exclusively to machines and converting the procedure into a machinelike automated procedure.

4.2. *Extraction of personal data from receipts, tax returns and public databases*

A significant measure in favour of the digitalisation of the taxation procedure is the recent conversion of the obligation to file documents and declarations - which are part of the tax legal relationship through accessory obligations - into a fully digital and dematerialised form. We are talking about the duty to file income tax returns, to file VAT returns, to issue invoices or to communicate relevant legal facts that are carried out through digital portals and in a totally dematerialised way.

This opens a set of possibilities and potentialities that cannot be negligible to the administration. The possibility for taxpayers to transmit information digitally (for example, scanned documents or electronic invoices) to the tax authorities allows the massive collection and processing of a huge amount of information. On the other hand, easily collected information is collected and stored in large databases, through easily manipulated media and can be easily translated and transmitted to foreign counterparts, within the framework of international agreements and European legislation in force. On the other hand, the processing of any huge text data associated with this is a task that cannot be

que la entidad sea más efectiva a la hora de prestar sus servicios y que estos tengan un mayor valor agregado. Hacer más fácil la vida de los ciudadanos en su interacción con el Estado mediante el uso de tecnologías digitales implica cambiar la forma de pensar". M. Llanes Font, M. Díaz De Ceballos and Y. Salvador Hernández, *Administración pública y cuarta revolución industrial. ¿Qué nos lleva hasta allí?*, in *XXXIII Concurso del CLAD sobre Reforma del Estado y Modernización de la Administración Pública "La cuarta revolución industrial en la administración pública*", Caracas, 2020, 10, avaliable at https://clad.org/wp-content/uploads/2020/12/Mención-Honor%C3%ADfica-Lorena-Mariluz-Llanez-et-al.pdf.

"Incorporar las tecnologías de forma instrumental, a saber, para cubrir el objetivo de la cuarta revolución industrial que favorece la gestión procesal en el menor tiempo posible y con el menor gasto". S. Barona Vilar, Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema?, in *Rev. Boliv. de Derecho*, No. 28, 2019, 39. "Nas últimas três décadas, o desenvolvimento das tecnologias de informação (TI) e a sua integração nos processos de produção trouxeram benefícios ao nível de toda cadeia de valor. A evolução na capacidade das tecnologias alavancaram a produtividade industrial, reduzindo os custos de produção e fornecendo soluções eficazes para atender os clientes com qualidade, velocidade e melhor custo/benefício. Atualmente, a introdução de novos conceitos como a produção baseada na Internet não só permite melhorar a comunicação entre fabricantes, clientes e fornecedores como cria maneiras de atender os clientes através de novos modelos de negócios". B. Santos, A. Alberto and T. Lima, *Indústria 4.0: Desafios e Oportunidades*, in *Revista Produção e Desenvolvimento*, No. 4, 2018, 112.

efficiently managed by human capacity.

Therefore, it is entirely appropriate that the procedure of collecting, processing, and extracting the information and data in these delivered documents should be automated to discover their value. A suitable and potentially applicable method for this is Text Mining.[16] Here, information can be extracted from both structured and unstructured data text files. The approach is used, for example in pattern extraction, as text mining analyses large amounts of data and helps identify patterns, or during literature examination, as the method can process the text in question, define its subject matter and/or highlight the most frequently used terms.[17]

In contrast to natural language processing, [18] here no semantic features are considered. However, the search for information patterns or the identification of corresponding structures can be carried out with text mining. Relationships between words in the text are shown, word frequencies and patterns used are analysed. Therefore, the procedure is an irreplaceable method for identifying statistical features. As a result of detail extraction, text mining enables the provision of accurate information from the text.

4.3. *The prevention of pathological acts*

One of the strategic objectives of the Tax Administration revolves around the promotion of compliance by taxpayers and the fight against tax evasion and fraud by those taxable persons who do not comply with their tax obligations. Improved compliance should be achieved through a wide range of core tasks of tax administration officials, including the investigation and detection of tax evasion and fraud.[19] To this end, it is necessary to carry out an exhaustive analysis of the results of the control actions of the effects that they induce in the taxpayers' fiscal behaviour, to achieve that the ideal of regularisation of tax obligations becomes an additional tool now of achieving an improvement in the voluntary fulfilment of those obligations.

The digitalisation of society as a whole and of economic activity specifically, are producing a significant change in the way the business sector and large organisations are organised, particularly in an economic and functional context. In order to respond to these new needs, the tax administration must implement mechanisms that allow structured information retrieval systems aimed at facilitating tax data relating to the control and supervision of acts in tax matters relating to income tax and VAT, in order to allow a more simplistic management of tax obligations, the restriction of the use of business information processing systems that allow the concealment of sales or activities, with a special focus on the activity of online platforms dedicated to the intermediation or direct sale of goods or services. Obtaining information, systematising, and analysing it, carrying out concrete activities or fostering national and international cooperation to act on this digital world that is constantly developing, and evolving is a necessity that cannot be neglected here.

In this way, the creation of ratios and risk indicators offers the Tax Administration bodies greater control, both in terms of encouraging compliance with tax obligations, and in terms of supervision and control over

[16] "Data or text mining" is the activity that involves collecting personal data using artificial intelligence systems and storing it in a bigdata context. By processing this data and converting it into computerized information, it will be possible to create statistical and mathematical methods that produce concrete results that are intended for application in certain contexts. It is essentially considered the ability to assess future conduct and based on statistics and probabilities, being assessed by virtue of presumptions created through probabilistic maxims based on purely mathematical criteria.

[17] Automated decisions and profiling emerge as one of the great technological advances of a post-modern and technological society. From the analysis of mega data and its automatic learning it is possible, by collecting information and understanding the profile of its holder, to formulate hypotheses and patterns that will be mathematically and statistically probable, understanding its routine performance and daily habits. Think of frequent donations, daily meals in a certain establishment, or the simple consumption of a coffee at the same time every day. By processing these personal data, it is possible to determine an assertive profile of the data subject and achieve certain interests that may be positive or negative for them. M.D. Masseno, *Como A União Europeia Procura Proteger os Cidadãos - Consumidores em Tempos de Big Data*, in *Revista Eletrônica do Curso de Direito da UFSM*, vol. 14, No. 3, 2019, 2, avaliable at https://periodicos.ufsm.br/revistadireito/article/view/41708.

[18] We refer, essentially, to the classic activity of manual information gathering and processing done by reading and storing the information, to be later applied and used in the corresponding administrative procedures.

[19] J. Calderón Carrero and J.S. Ribeiro, *Limites ao uso da inteligência artificial no controlo fiscal: a experiência francesa (Decision No. 2019-796 DC)*, in *Cadernos de Justiça Tributária*, No. 26, 2019, 3.

the true contributory capacity of the same in relation to what has been declared. It is in this field that big data and artificial intelligence prove to be a real asset in the management of this data analysis and in the automatic performance of acts that prove to be convenient for the intended purposes, achieving a swift and efficient action in relation to the data processed and the results intended to be achieved. Thus, whenever the intelligence systems detect signs of non-compliance that are clear, it will be entirely appropriate for the same to act in conformity with what is appropriate, counteracting the harmful effects resulting from non-compliance or omissions.

In the context presented, it should be noted that bigdata and social analytics will seek priority action in a set of tasks that will allow an improvement in strategic sectors in the fight against tax evasion and fraud, namely:

1) Information sources and technological advances aimed at risk analysis, which are the basis of any taxpayer selection process. To this end, planning processes will be necessary that act on different sources of information, both domestic and international, to strategically facilitate the selection models of the data obtained by the Tax Administration. At international level, in view of the new international standard for the exchange of information driven by the Global Forum on Transparency in tax information, automatic models for the exchange of tax information are gaining increased importance, enabling important analysis and optimization work to be carried out on the tax information obtained, in order to ensure greater transparency, which is intended to become a reality and consequently lead to greater difficulty in concealing assets and wealth, so as to ensure the correct taxation and declaration of existing and previous wealth of different financial assets located abroad. The information received by the Tax Administration has been gradually increased due to the presentation of the so-called "country-for-country", to prevent the erosion of tax bases and the transfer of benefits (BEPS) to more fiscally favourable States, countries, or territories. Also, the models implemented by the Council Directive 2016/881 of 25 May 2016, whose focus was directed to large multinationals, collects many activities as to the territories in which they operate. Based on this data, it is possible to create profiles and risk detection systems that systematise and delimit risks and allow for better monitoring of these risky activities.[20] [21]
2) Controls of internal taxes through automated systems of risk analysis on transfer pricing based on a whole range of information available on related transactions that the Tax Administration currently has, making effective use of the data and information available to the inspection means because of the BEPS project, both within the scope of the OECD and the European Union, among which we highlight the procedures for automatic exchange of information on various facts.
3) Control in relation to the granting and maintenance of tax benefits, making it possible to verify applications for the granting of tax exemptions or benefits, as well as their maintenance. This will seek to intensify control activities aimed at proving proper compliance with the specific requirements laid down for the correct application of the special tax regime that grants these benefits and exemptions. Control in the taxpayers' actions and in the analysis of information, since the economic activity has in recent years been in a constantly evolving environment, deserving the analysis of business models by the Tax Administration, which cannot neglect the activity of those with a higher tax risk profile. It is axiomatic that there is a need to consolidate the different ways of

[20] "Tax information, which often includes a taxpayer's income and other details about an individual's personal circumstances, is a particularly sensitive form of personal information. Tax information may reveal, among other things, information about income, spending and savings, employment status, personal belongings, disability status, associations and club memberships, donations to charities, mortgage costs, child support and alimony, and the amount and size of gifts to family members and others. This detailed personal information may be used to construct a detailed profile of an individual's identity, including her religious beliefs, political alliances, and personal behavior". A. Cockfield, *Protecting Taxpayer Privacy Rights Under Enhanced Cross-Border Tax Information Exchange: Toward a Multilateral Taxpayer Bill of Rights*, in *University of British Columbia Law Review*, vol. 42, 2010, 42, especially 437.

[21] E. Politou, *Profiling tax and financial behaviour with big data under the GDPR*, in *Computer Law & Security Review*, vol. 35, No. 3, 2019, 306, especially 307; D.E. Holmes, *Big data: a very short introduction*, Oxford, Oxford University Press, 2017.

obtaining information which provide information on the amounts, nature and identification of the parties involved in the commercial relationship in a wide range of economic activity. The required data is thus necessary for the Tax Administration to perform an exhaustive control of the correct taxation of these businesses, avoiding harmful conducts of tax evasion and fraud.

These guidelines or interventionist maxims that the Tax Administration has been marking, considerably, the functional activity of the Tax Administration, revealing a migration to an activity eminently dependent on personal data and on the use of computerized and automated means, seeking in the various matters to take advantage of these for a better efficiency of the functional activity and the achievement of the results to be pursued.[22] But the common denominator to all these concrete directives where the analysis of a large volume of information and the automated processing of data allows the Tax Administration to act better resides in the personal data and the ways in which they are obtained, in this case, the automatic exchange of information procedure being one of the most relevant mechanisms and instruments.

5. *Conclusion*

So as can be seen, the rise of artificial intelligence systems and the consequent mechanisation of administrative procedures is today an undeniable reality. The ease of application and the benefits that are obtained through the "machining activity" of administrative procedures bring us two conclusions that prove to be indisputable, and which we should assume without hesitation.

The first conclusion arises from the need that administrations must adopt procedural mechanisation systems. The phenomena of globalisation, the opening of markets and the complexification of relations between subjects and public and private entities have brought about a clear paradigm shift. What was previously considered sufficient according to the rules and relationships established, today, these instruments are clearly insufficient.

The second conclusion to be drawn is that the artificial intelligence systems, allow an optimisation and rationalisation of the available means, enabling a better performance of the existing mechanisms, reaching maximum administrative efficiency and effectiveness that improve the administration's activity.

But, because we cannot fail to consider only the positive aspects, we must start from the assumed positivity's to, in articulation with other studies, identify the negative points that must be considered when integrating these systems of artificial intelligence. Aspects such as the dignity of the human person, the right to informative self-determination, or the right to privacy of the subjects are legal realities that must be considered. To neglect this is to assume only one vertex of a long pyramid. Therefore, it is up to the academy and scholars to identify and study concrete measures that allow a proper articulation and respect for all those involved, respecting what is essential and central to the social and legal order: the human being.

[22] J.M. Freitas Da Rocha, *A administração tributária odiosa (repensando os fins e atuações do fisco)*, 7, avaliable at https://repositorium.sdum.uminho.pt/bitstream/1822/61950/1/AT%20odiosa.pdf; J. Casalta Nabais, *O Princípio da Legalidade Fiscal e os Actuais Desafios da Tributação*, in *Boletim da Faculdade de Direito*, Volume Comemorativo, Coimbra, Universidade de Coimbra, 2003, 1008; A.F. Brás Carlos, *Impostos, Teoria Geral*, Coimbra, Almedina, 2010, 162; N. De Sá Gomes, *Lições de Direito Fiscal*, in *Cadernos de Ciência e Técnica Fiscal*, Centro de Estudos Fiscais, Direção-Geral das Contribuições e Imposto, Ministério das Finanças, vol. II, No. 134, 151; F. Peña Álvarez, *Princípios de la Imposición em uma economia abierta*, in *Manual de Fiscalidad Internacional*, III ed., vol. I, Instituto de Estudios Fiscales, Escuela de Hacienda Pública, 68.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 151-158
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 13

*The Responsibility in Automated Administrative Decisions**

Adriana Ciafardoni
(PhD student at the University of Modena and Reggio Emilia)

ABSTRACT This paper dwells on the issue of responsibility in automated administrative decisions. From this perspective, on the one hand, the participation of the administrative official is considered as necessary – even simply in terms of supervision and control – in the case of procedural activities executed by software and, on the other hand, it is necessary to question the possibility of resorting to the organic theory to face decisions' attribution problems is explored.

1. *The automated administration: an overview*

The reasoning about administrative decisions in a future-oriented perspective implies the need to consider the possible use of technology and challenges of the algorithmic society. The need to implement the use of technology in the public sector has been particularly felt, for its potential to increase accessibility, security, efficiency, transparency and simplification.[1] Indeed, the algorithm is the focus of a new debate on the possible use of new technologies in the legal field. The potential of the digital revolution has attracted a growing interest since, in recent years, the interaction between technical-scientific knowledge and social structures has increased. In various sectors, algorithms are identified as instruments of redemption to correct systematic distortions, exclude human emotions and errors, take neutral and efficient decisions and improve the overall administrative action. Human beings' debatable evaluations can be replaced with objective and rational machines' choices, that are characterized by an intrinsic neutrality.

In this way, there would be less errors and doubts and the general distrust in human choices would also disappear. Benefits increase even more with regard to public authorities, since the particular status of the administration originates an idyllic search for impartiality in the fulfilment of choices and assessments. In other words, algorithms would make possible to create a perfect administration.

Nevertheless, a different and much critical orientation about society's robotization has made its way, not excluding the wide scope of digitalization, but circumscribing its benefits. Indeed, even the use of algorithms imposes some evaluations in the choice of relevant data, selection criteria or models to be developed. These choices are not neutral or irrelevant and influence the final robotic decision. In fact, every action (consciously or unconsciously) taken by a human being who works alongside the software inevitably influences it. Thus, also algorithms that have been established to exclude human choices, requires subjective evaluations for their operation.

All of this means that human discretion is not nullified, but simply changes in its form, assuming relevance in the algorithm programming and in the data choice.

However, the use of algorithms requires something more than a mere digitization[2] since the technology is not used to shape a decision taken by the public administration, but to determine its content.[3] In fact, the application of an algorithm is quite different from the digitization.[4] This last phenomenon

* Article submitted to double-blind peer review.

[1] M.A. Sandulli, *Il procedimento amministrativo e la semplificazione,* in *Jus publicum*, No. 4, 2012, 57. According to the author, interventions designed to streamline and simplify the administration must not be limited to the possibility of using legal instruments provided for and applicable in the procedure. In fact, it must also be possible to use other instruments that can lead to a concrete simplification, such as the use of telematics, because computerization is equivalent to simplification. See also, A.G. Orofino, *La semplificazione digitale*, in *Il diritto dell'economia*, No. 3, 2019, 87.

[2] On the distinction between digitisation and algorithms, see A. Simoncini, *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico,* 2019, 1149.

[3] Like this, A. Simoncini, *Profili costituzionali della amministrazione algoritmica*, 1167.

[4] For S. Del Gatto, *Potere algoritmico*, *digital welfare state e garanzie per gli amministrati. I nodi ancora da sciogliere*, in *Rivista italiana di diritto pubblico*

has been in progress for a long time and is also well underway. The digitization started to emerge in the *Rapporto Giannini* of 1979, in which it was hoped that "electronic processors" would be used to reorganize the public administration.[5] Therefore, digitization can only be the starting point for the automation, that consists in a much more complex procedure, with new variables.

For this reason, nobody has the intention to suggest that the robotization is already realized[6] and lawyers only have to try liming further damages or, at least, containing them using the secure garb of legal legitimacy. On the contrary, there is a need for studies aimed at circumscribing robotization's limits within the meshes of reassuring constitutional guarantees.

The algorithm's application lends itself to possible criticalities that concerns, on the one hand, technical and human resources and, on the other hand, procedural guarantees.[7]

With regard to the first issue, an investment in structures and human capital is needed, so that computerized decision-making processes can be implemented. Indeed, the introduction of new technologies must be supported by appropriate investments. In this sense, it is necessary to apply some changes to the public apparatus: one cannot speak, on the one side of digital and digitized public administration and, on the other side, of "another" one. Moreover, significant investments in technological innovation and digitization are made possible by the National Recovery and Resilience Plan (PNRR) and allows to implement smart policies and actions for the development of public administration's information technology.[8]

Concerning the second issue, procedural guarantees and the protection of individual rights in algorithmic decisions must be left unprejudiced, setting the benchmark on the principles of responsibility, transparency, legality, non-discrimination and participation.[9]

Therefore, it is necessary to balance opposite demands: those related to the efficiency and simplification of the administrative action and the ones linked to the protection of individuals and involved public interests. This is because digitization cannot be imposed in breach of general principles of administrative law, which must form barriers against new forms of automated measures. Thus, it is required to start a transformation process that allows to adapt computer software to constitutional requirements and citizens' full protection, even if it implies a revise (*rectius*: rethink) of the administrative organization.

2. *The principle of responsibility and the automated administrative decision*

The issue of the robotization of the public administration (and its choices) should not be separated from a prior discussion on the responsibility, that consists in a necessary and indispensable condition for speaking of automatized choices,[10] even abstractly.

In this perspective, it is necessary to focus on two circumstances: why and how talk about responsibility in respect to the use of algorithms in automated decisions, that is, which responsibility imputation model it is needed to be adopted. This is because the responsible entity for decisions taken, and acts adopted through an algorithm constitutes a necessary condition in western democracies: it is not possible to speak of the rule of law without an appropriate system of responsibility attribution.[11]

With regard to automated decisions, it is necessary to avoid two antithetical situations: one that would lead to an always responsible administration and the other that would steer

comunitario, No. 6, 2020, 830, algorithms and computer systems that process big data go beyond the mere digitization, changing the public administration from within. This is because they change the way in which decisions are made and public policies are developed.

[5] See A. Simoncini, *Profili costituzionali della amministrazione algoritmica*, 1166.

[6] This expression refers to R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Diritto amministrativo,* No. 2, 2020, 305.

[7] In this sense, M. Simoncini, *Lo Stato digitale. L'agire provvedimenale e le sfide dell'innovazione tecnologica*, in *Rivista trimestrale di diritto pubblico*, No. 2, 2021, 530.

[8] The mission 1 of the National Recovery and Resilience Plan "digitisation, innovation, competitiveness, culture and tourism" has a total budget of €40.32 billion, of which €9.75 billion is reserved for digitisation, innovation and security in the public administration.

[9] M.C. Cavallaro and G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi*, 2019, 19.

[10] On the centrality of this issue in the legal context, see A.G. Orofino and G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione,* in *Giurisprudenza Italiana*, 2020, 1745.

[11] See C. De Nicola, *Illecito del dipendente e imputazione della responsabilità alla pubblica amministrazione*, in *Diritto amministrativo*, 2021, 917.

the system away from responsibility.[12] We could not even abstractly talk about administrative automation without clarifying, with reasonable certainty, who is to be held responsible and in which terms. The basic problem, however, is that today there is a logical inversion in the relationship between legal categories and innovations. That is, first new technologies are applied, and then problems that arise each time are framed in existing legal categories. Moreover, this path must be reversed, at least for what concerns responsibility. We cannot use machines and identify the person responsible after the damage has occurred, and this is also (and above all) to guarantee citizens who must know in advance who they can act against.

The starting point consists in the principle of responsibility and the existing constitutional framework.[13] The article 28 of the Italian Constitution establishes officials' responsibility for acts committed in breach of rights. Results to be unquestionable the interpretation according to which, despite the literal fact, there is a direct responsibility of the administration as a result of the application of the theory of organic identification. Thus, although acts are materially adopted by the public official, both acts and effects are attributed to the administration, by means of the relationship of identification between the organ and the public body.

Clearer is the provision contained in the Article 97 of the Italian Constitution, in which, in addition to the legal reserve that ensures public administration's impartiality and good performance, it is specified that officials' spheres of competence, powers and responsibilities are established in the organization of offices.

Therefore, the Italian Constitution requires a link between the responsibility for the adoption of an authoritative act and a public official, for the obvious reason that an act capable to affect unilaterally the legal sphere of individuals must always be controlled by public authorities, through the participation of the public official in the decision. Moreover, this control attributes responsibility to the public administration, using the theory of organic identification. This is particularly important for algorithms' use. In fact, the robotization of the administration pursues, the opposite need: that is, to remove the human contribution from the decision, in the idyllic belief that replacing human beings' debatable evaluations with machines' objective and rational choices can lead to a neutral and efficient administrative action.

However, the Constitution sets a limit on the use of automated choices, requiring that there must be a link between the act and the official. It follows that robotization should be excluded, whenever it is not possible for a person belonging to the administration to intervene in the decision, even in terms of supervision and control. In other words, automation should be allowed only if it is possible to have an effective intervention of the official, with respect to the automated decision.[14]

In this sense, it is referred to the principle of non-exclusivity of the algorithmic decision, that derives from the provisions of Article 22[15] of the General Data Protection Regulation (GDPR) and is also accepted by national and EU case law.[16] In fact, judges of the Council of State, require a human contribution in the decision-making process, capable of checking, validating or refuting the automatic decision.[17]

[12] A.G. Orofino and G.R. Orofino, *L'automazione amministrativa: imputazione e responsabilità*, in *Giornale di diritto amministrativo*, No. 12, 2005, 1306, underlines that it is necessary to establish some criteria for the attribution of the responsibility, in order to avoid a kind of depersonalisation of the administrative action by means of computers, that allows to escape from responsibility.

[13] For a deeper view, M.C. Cavallaro, *Immedesimazione organica e criteri di imputazione della responsabilità*, in *P.A. persona e amministrazione,* No. 1, 2019, 41.

[14] I.M. Delgado, *La riforma dell'amministrazione digitale: un'opportunità per ripensare la pubblica amministrazione*, in L. Ferrara e D. Sorace (eds.), *A 150 anni dall'unificazione amministrativa italiana*, Florence, Firenze University Press, 2016, 133, the author clarifies that the presence of an automated decision – moreover, even if there is no contribution by a person – it does not imply that the authorship of the act is attributed to the algorithm, always having to fall on the administrative body that holds the power and exercises it.

[15] "The data subject has the right not to be subject to a decision based solely on automated processing".

[16] Council of State, Sec. VI, 13 December 2019, No. 8472 and Council of State, Sec. VI, 4 February 2020, No. 881, according to which there must in any case be a human contribution in the decision-making process capable of checking, validating or refuting the automatic decision. In mathematics and computer science, the model is defined as HITL (human in the loop), in which it is necessary that the machine interacts with the human being, in order to produce its result.

[17] Council of State, Sec. VI, 13 December 2019, No. 8472 and Council of State, Sec. VI, 4 February 2020, No. 881.

In application of this model, known in informatics as human in the loop (HIDL), human participation in the machine's activity is indispensable for the final result.[18] In this sense, one can understand the need to recover (*rectius*: preserve) the human element in administrative decisions, in order to safeguard their increasingly necessary dignity.

However, the European formulation of the non-exclusivity principle and the one of the national case-law do not completely coincide, since the orientation adopted by local judges tends to be more flexible, considering human participation as sufficient, even if only in terms of control and supervision. In any case, the intention of the European legislator is to exclude the admissibility of fully automated decisions. This has a central role in the relationship with the principle of responsibility and makes it indispensable for individuals belonging to the public administration, to assess compliance with legal parameters and consistency between the model used and the intended one.

However, an effective control is not always possible, and it is important to prevent the creation of an absolute-responsibility system, which would always bring the administration to account even if the public official could not carry out a check or a verification, even abstractly. In this sense, the Italian Constitution sets a limit on the use of the algorithm. In fact, if it is not possible to trace the act back to the official, due to impossibility of carrying out controls, the automated decision should be excluded.

To better understand the foregoing, it is necessary to start from a twofold consideration: the first concerns the type of decision that the machine could adopt, and the second concerns the type of algorithm that can be used.

Regarding the first question, the algorithm could be adopted for serial and standardized procedures (constrained activity) or with respect to discretionary activity. The exercise of the bound power requires only the unambiguous identification of assumptions followed by predetermined results. In this sense, the automated procedure is well suited to handle necessary steps, speeding up procedures and reducing their duration. This would become particularly complex in the hypothesis of discretionary choices, since it would be necessary to implement a comparative evaluation of several interests, in order to enforce the final decision. In this way, the algorithm could play a role that is not only limited to the impersonal collection of data necessary to make a binding decision, being able to constitute a system for the formation of the procedural will itself.[19]

With regard to the second question, making the discourse as simple as possible, the term "algorithm" refers to a clear and unambiguous set of instructions drawn up to solve a problem.[20] In this sense, it is only able to execute entered commands, in order to automate procedures. In other words, it operates in an objective sense: the same inputs will always produce the same outputs.[21]

Alternatively, the algorithm can interact with artificial intelligence systems[22] and this makes possible to develop a self-learning software. The algorithm is able to make "intelligent" choices autonomously. In fact, the use of so-called machine learning means that the algorithm, which has a good degree of controllability, can develop its own

[18] This model has been positively accepted in doctrine, *ex multis,* E. Carloni, *I principi della legalità algoritmica*, in *Diritto amm*inistrativo, No. 2, 2020, 294; V. Neri, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urbanistica e appalti*, No. 5, 2021, 581; M.C. Cavallaro, *Imputazione e responsabilità delle decisioni automatizzate*, in *European Review of Digital Administration & Law*, vol. 1, issue 1, 2020, 70; A. Simoncini, *Profili costituzionali della amministrazione algoritmica*, 1186. The latter author points out that human participation in algorithmic activity is inevitably influenced by ethical principles that must govern the use of machines.

[19] M.C. Cavallaro and G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, 16.

[20] In this sense, *ex multis*, P. Ferragina and F. Luccio*, Il pensiero computazionale. Dagli algoritmi al* coding, Bologna, Il Mulino, 2017, 10.

[21] G. Gallone, *Il Consiglio di Stato marca la distinzione tra algoritmo, automazione ed intelligenza artificiale*, in *Diritto dell'internet*, No. 1, 2022, 163. In particular, the Author starts from the judgment of the Council of State of 25 November 2021 No. 7891 and dwells on the distinction between "traditional" automation, that is the mere use of algorithms, and "advanced" automation, through the use of artificial intelligence systems.

[22] The first studies on the application of artificial intelligence date back to the Dartmouth Conference in 1956. On the characteristics of artificial intelligence in the modern context, D. Marongiu, *L'intelligenza artificiale "istituzionale": limiti (attuali) e potenzialità*, in *European Review of Digital Administration & Law,* vol. 1, issue 1-2, 2020, 37. For a careful analysis of new risks for public authorities, see A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law*, 2020, vol. 1, issue 1-2, 63.

"consciousness". The reason is that, if for what concerns the mere software, consequences are predictable given the assumptions, with the use of artificial intelligence programs are not limited to commands' execution but become part of the formation of will: they shape the given rules, producing new ones.[23]

In the light of the above, it is clear that the use of the algorithm seems to be sufficient, with respect to constrained activity. In fact, the solution offered by the algorithm is standardized: once identified relevant data, for identical cases the decision will be the same. In such a case, the algorithm is controllable. In fact, once premises have been established, consequences are predetermined, so that verification by the official or the person responsible for the procedure is possible.

When applied to discretionary choices, this mechanism is insufficient. Hence the need to supplement the algorithm with recourse to artificial intelligence, with the consequence that decisions may not be controllable or predictable by the administration nor by the programmer, since there will be a progressive and ever-increasing distancing of the program from the person who chooses. Beyond possible future developments of artificial intelligence, it should be noted that systems adopting this model led to the loss of effective control over the software.[24]

In this last case, it is necessary to verify the concrete possibility of an intervention of the public administration and if the damage would be represented as certain in any case, regardless of the officials' degree of diligence and the intervention envisaged; then, the use of machines would be unconstitutional, insofar as taken decisions are not verifiable. Moreover, there would be also the problem of justifying a choice, if it differs from a possible investigation carried out by an individual, without having fully understood its reasons.[25]

This is not a preclusion for automated administrative decisions, even in the case of discretionary activity. Apart from the aim to limit the administration's robotization, a control on a self-learning system is particularly complex. Without considering computer skills, it is easy to see that if (and only if) the official is unable to control and verify the work of the machine, there would either be absolute responsibility, without no control possibility, or there would be no responsibility at all. This would also be inadmissible in practical terms, because no administration would assume responsibility for an incontrollable act, capable of affecting legal situations of private individuals. Moreover, no legal system could admit the creation of a grey area, in which the administration would not be responsible, even in the presence of authoritative acts. Alternative solutions, such as a programmer's responsibility,[26] are not even abstractly conceivable with respect to an authoritative act[27]. As perhaps ironically stated in a Resolution of the European Parliament of 16 February 2017 on the relationship between robots and civil law, we would be forced to enhance machines' decision-making autonomy.[28] There is a need to balance the

[23] G. Gallone, *Il Consiglio di Stato marca la distinzione tra algoritmo, automazione ed intelligenza artificiale*, 163.

[24] A. Matthias, *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics and Information Technology*, No. 6, 2004, 182.

[25] See S. Del Gatto, *Potere algoritmico*, *digital welfare state e garanzie per gli amministrati. I nodi ancora da sciogliere*, 481.

[26] For a different but interesting solution, see E. Picozza, *Politica, diritto amministrativo and artificial intelligence*, in *Giurisprudenza italiana,* 2019, 1657. According to the Author, it is possible to attribute responsibility for omissive or negligent conduct of the A.I. to its programmer and maintainer: in such a case, however, the software engineer who 'drives the machine' objectively becomes a public official with all related consequences, including the accounting responsibility case before the Court of Auditors for financial loss; if, on the other hand, one opts for a 'direct' responsibility of the machine towards third parties (as normally happens in a 'real' administrative office), the responsibility of its programmer and maintainer would still be a civil and recourse responsibility.

[27] A.G. Orofino and G.R. Orofino, *L'automazione amministrativa: imputazione e responsabilità*, 1308. According to the Authors, there are three moments of imputation of responsibility: the first concerns those who decided on the programming criteria; the second concerns those who dealt with the investigation phase; the third concerns those who are competent to adopt the act.

[28] D. Di Sabato, *Gli smart contracts, robot che gestiscono il rischio contrattuale*, in *Contatto e impresa*, No. 2, 2017, 388. More recently, there are interesting suggestions in S. Civitarese Matteucci, *«Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità*, in *Diritto pubblico*, No. 1, 2019, 5. The Author underlines that there are computer techniques that are able to replicate different humans' cognitive capacities and the possibility of machine learning. Moreover, G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Diritto dell'informazione e dell'informatica*, No. 3, 2021, 342, underlines that in certain circumstances machines' cognitive capacities can exceed those of humans, taking

pursuit of celerity, efficiency and cost reduction (is this feasible today?) with the constitutional principle of public administration's accountability. The Constitution precludes the use of uncontrollable automated choices, insofar as they indirectly lead administrative acts back to the employees.

Therefore, the principle of responsibility could (and should) represent the deadline between a legitimate and possible recourse to the algorithm and an impermissible one. In fact, if an effective control on the decision adopted by the official becomes necessary, also in terms of supervision, then the same must be possible, at least abstractly. Obviously, there is a need to improve human capital's skills, because the legal training of public officials is no longer sufficient.

The paradox is that, in no time, jurisprudence has gone from limiting the use of the algorithm to the mere exercise of the bound power[29] to find no reasons of principle, or rather concrete ones, for limiting the use of technology of bound administrative activity, rather than discretionary one,[30] even if the reason can be found in the principle of responsibility.

Therefore, another aspect must be emphasised[31]: after clarifying the need of human control, avoiding that the decision remains at the mercy of machines – need which derives from the Constitution and is accepted by the case law – it is necessary to question if, today, the abovementioned control is possible and effective and admit automated decisions only within these limits. This does not exclude the possibility that actual margins of intervention may increase, even in the short terms, with the science evolution. Therefore, with respect to the use of artificial intelligence – and to all systems that want to exclude human intermediation – a concrete control is necessary to assess the possibility of intervening in the decision, if an absolute preclusion is not to be envisaged.

3. *The model of responsibility*

After clarifying the need to track the responsibility to the Public Administration and the official, a second question arises: which system should be adopted to attribute the responsibility of the public body for the offence committed in case of automated decisions?

There are two possible solutions: the traditional theory of organic identification, with respect to which it should be questioned whether it is also suitable in relation to algorithms, as an alternative to the system of strict responsibility of the Civil Code.

The discourse on the organic identification is now well known and, according to this theory, acts are considered as carried out by the public body, although if they are materially adopted by the official. Therefore, there is no difference between the individual who acts and the body in which he is incardinated, hence officials' activity is imputed to the administration. In this case, the question is whether to attribute to the organ also machines' activity, in the hypotheses that the person limits himself to carry out supervisory and control tasks, acting through the organ. Therefore, would the organ remain the centre of imputation of the machine's acts even if officials do not materially take the decision, but they merely carry out a control?

The alternative would be to resort to systems of objective responsibility.

The possibility to track back responsibility to the Article 2051 of the Italian Civil Code is suggestive, because this rule is inspired by the need for distributive justice, according to which it is not permissible that consequences caused by inanimate things fall on an innocent person, rather the responsibility is of the person who holds or uses the *res*.[32] In this way, the machine is considered for what it really is: a thing, a tool at the service of the administration (an excellent tool, but, however, one of many). In this case, it is necessary that the thing is included in the causal sequence that led to the harmful event, in order to establish the responsibility of Public Administration. Moreover, following the case law, the requirement of dangerousness occurs both if the object has an intrinsic dynamism – that is, dangerous in its

from data imperceptible or hardly detectable information.

[29] Council of State, Sec. VI, 8 April 2019, No. 2270.

[30] Council of State, Sec. VI, 13 December 2019, No. 8472 and Council of State, Sec. VI, 4 February 2020, No. 881.

[31] Council of State, Sec. VI, 13 December 2019, No. 8474, where it is stated that there aren't reasons of principle, or concrete reasons, for limiting the use to binding rather than discretionary administrative activity, since both are expression of the authoritative activity carried out to pursue the public interest.

[32] Civil cassation Court, 31 May 1971, No. 1641.

functioning – and if the interaction with the damaged party is *a condicio sine qua non* for the event. The algorithm is not dangerous, but it could be, since it is capable of producing damages. It follows that the administration would be responsible both for the damage that depends on an intrinsic situation of the thing (a defective program) and for a harmful element arising in the thing (criteria established by the administration for the automated choice are discriminatory).

This does not seem to be such a negative solution, at least on a first reading. Moreover, since responsibility is objective, the private party is not called upon to prove the subjective element, which is not simple in a technical and complex situation such as the use of machines. The problem has arisen because jurisprudence admits the administration's responsibility for breaching custody obligations, even regardless of possibilities of an effective control, if the damage is caused by intrinsic reasons to the thing.[33] This, compared to an automated decision, would mean an administration that is always accountable.

From the above explanation derives the need to resort to the theory of organic identification,[34] which is to be deemed possible and is today also the most reassuring choice, since it is the solution accepted by case law. This is because accepting this model would not distort the system of responsibility imputation to Public Administration, since the case law of the Council of State underlines the need to attribute the decision to the organ holding the power, which must be able to carry out the necessary verification of the choice's logic, its legitimacy and the results entrusted to the algorithm.[35]

Moreover, if the theory of organic identification represents the theoretical scheme by virtue of which the public administration becomes the imputation centre of acts carried out by a natural person, this model is also the most suitable if the act is referable to a person, even though it is carried out by the machine.[36]

The problem arises if an official's control is not possible, in which case the applicability of the organic theory would seem to be precluded upstream. In fact, the acts on which the official must carry out a check can be attributed to the Public Administration, even if with a slight forcing; the hypothesis of acts taken 'in conscience and autonomy' by the machines is different, since they are not attributable to public powers, for this reason. Therefore, if someone chooses to impose human participation in decision-making processes, as required by the Italian Constitution, then organic identification is (still) suitable to address the problems of imputation.

4. *Brief conclusions*

In light of the above, each time it is objectively impossible for the authority to exercise a power of control over the decision the responsibility should be excluded, considering the specific situation. In fact, the responsible for the procedure or the manager responsible for an act must always control the procedure for the formation of the will, in order to analyse eventual results of resorting to the algorithm.

This is because the adopted act must comply with national and international law, with the principles of reasonableness, proportionality and non-discrimination, be clear and, therefore, accessible to the community. It follows that if official's control is not possible, the administration cannot be liable because it would have no real possibility for the prevention of damage.

On the other hand, it would be utopian to ignore that the mankind is far from being replaced by robots and that the actual evolution of science cannot cause most of the problems that today (rightly) catch legal scholars' attention.

Moreover, the principle of responsibility implies the need to maintain the official's control over the software, if applied to automated administrative decision-making processes. In this sense, the public administration is a servant – and not supporting – element of the administration, keeping on public authorities the competence

[33] Civil cassation Court, 15 October 2019, No. 25925.

[34] In general, on the theory of organic identification, M.C. Cavallaro, *Immedesimazione organica e criteri di imputazione della responsabilità*, 39.

[35] Council of State, Sec. VI, 4 February 2020, No. 881 and Council of State, Sec. VI, 13 December 2019, Nos. 8472, 8473 and 8474.

[36] Indeed, there is no reason to exclude the responsibility of the administration if it is used an algorithm to make the final decision. On this issue, A.G. Orofino, *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in *Il Foro amministrativo CDS*, 2002, 2263.

and the control over the decision.[37]

Therefore, the public administration must carry out a twofold verification: on the one hand, to supervise machine's operations and, on the other hand, to identify necessary prerequisites for the algorithm. In fact, the prerequisites' identification implies some consequences. Algorithms have the power to enable and assign significance to relevant circumstances, because different assumptions can lead to different decisions.

Obviously, this would partly shift the problem. The question would not be who or why is liable, but where to place the divide between a controllable automated decision and an uncontrollable one. Alternatively, the judge would be called upon to assess the legitimacy of machines' use in the concrete case and, whenever the automated act could not be traced back to a person belonging to the public administration, even indirectly, it would be null and void because it would contravene to mandatory rules requiring compliance with the principle of responsibility.

This is because the alternative to such a (albeit problematic) balancing act would be the decline of the use of artificial intelligence, even before the era of automated decisions really comes. For the obvious reason that no public administration would take responsibility for uncontrollable decisions, the so-called defensive administration would reach its extreme consequences, in such cases. Alternatively, there would be the opposite solution: a total lack of responsibility for public authorities, a grey area without control. In other words, if uncontrollable decisions were allowed, this would legitimize either an administration that always responds or a never responsible one.

Therefore, with respect to a necessary administration-machines integration, the limit must be found in the Constitution and, therefore, in a responsible administration, because it is the basis of progress and denying it would be anachronistic. This would be a benefit for all: for citizens, who are protected since they can take action against the administration, in any case and for any eventuality; for public officials, who would be called upon to verify only what can be verified; for the public administration, which would not be responsible in an absolute way and without any limit (when the administration pays, citizens pay); for the digitization of society, with respect to which, if we do not set limits, we would end up stopping and destroying it, losing any possible future benefit.

[37] In this sense, M.C. Cavallaro and G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, 21.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 159-165
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 14

*The Conseil d'Etat Finds the Use of Facial Recognition by Law Enforcement Agencies to Support Criminal Investigations "Strictly Necessary" and Proportional**

Theodore Christakis
(Professor of International and European law – Université Grenoble Alpes & Director of the Chair on the Legal and Regulatory implications of AI)

Alexandre Lodie
(Doctor of International Law – Université Grenoble Alpes & Research Fellow – Chair on the Legal and Regulatory implications of AI)

French Council of State, *Decision n. 442364, 26 April 2022*

The Conseil d'État dismissed a legal challenge initiated by the French NGO "La Quadrature du Net" which claimed that the use of facial recognition by law enforcement agencies in criminal investigations to help identify suspects who appear in the TAJ System ("Traitement des antécédents judiciaires" - Criminal Case History Database) did not meet the EU Law Enforcement Directive's "absolute necessity" and proportionality requirements. In this case the French NGO "La Quadrature du Net" (LQDN) asked the French Supreme Administrative Court to invalidate article R 40-26 of the code of criminal procedure which expressly provides for the use of facial recognition to aid in the identification of suspects during criminal investigations. LQDN considered that the use of this technology was not "absolutely necessary" as required by the French version of Article 10 of the Law Enforcement Directive (LED). The Court dismissed this claim considering that given the vast amount of data contained in the TAJ database, the automated data processing was absolutely necessary. This decision feeds into the debate about how to interpret the strict necessity requirement laid down by the LED concerning the use of facial recognition.

ABSTRACT In this case the French supreme Administrative Court (Conseil d'Etat) was seized by a French NGO called 'La Quadrature du Net'. The NGO asked the Court to overturn the French Prime Minister's implicit decision to refuse to repeal some provisions of Article R 40-26 of the French Code of Criminal Procedures which enable the use of Facial Recognition by Law enforcement authorities to support criminal investigations. The Court dismissed this claim, arguing that these provisions are strictly necessary and proportionate to the aim pursued and thus compliant with the law enforcement directive.

1. *Setting the scene*

The use of facial recognition for crime prevention, investigation and repression has been under the spotlight for many years in France. In particular, the French NGO LQDN, which is a privacy and a numerical rights advocate, has repeatedly spoken out against the deployment of what it considers an intrusive technology.[1] One of the main targets of the LQDN's criticism has been the "Traitement des antécédents judiciaires" (TAJ), which is a police criminal case history database provided for by a 2012 decree,[2] which became operational in 2013. A new article was inserted into the code of criminal

* Article submitted to double-blind peer review.

[1] Facial recognition of demonstrators is already authorised, in *La Quadrature du Net*, 18 November 2019, available at: www.laquadrature.net.

[2] See Decree 4 May 2012, No. 652 concerning the processing of criminal record, available at: www.legifrance.gouv.fr/loda/id/JORFTEXT000025803463.

procedure as a result of this decree, which expressly provides law enforcement authorities with the option of retaining photographs of suspects or criminals for face matching at a later date via facial recognition software.[3] In other words, the system allows for the probe image of a suspect (from video surveillance footage or photographs) to be compared with images stored in the TAJ database (1-M).

As indicated in the TELEFI Report of October 2019, "the number of facial images on the TAJ was approximately 6 million out of which more than 99% were controlled images of suspects and victims (i.e. unknown dead bodies, the seriously injured and missing persons) whilst the rest (approximately 6000) were uncontrolled images (e.g. photo robot sketches, surveillance images etc.)".[4] The TAJ is populated with images that are captured and registered by the two police organisations in France, the National Gendarmerie and the National Police. Facial recognition is solely used as an investigative tool by investigators who perform searches. The law enforcement agencies and the Ministries of the Interior and Justice in France insist that such search results are used for operational purposes to support investigations, and not as evidence in court. The search results return a list of candidates, which is manually evaluated by the investigator conducting the search in order to decide whether the list contains a candidate likely to have been involved in a particular crime.

According to the TELEFI Report, "in 2018, approximately 200 000 searches were performed and a further 250 000 took place during the first eight months of 2019".[5] This system enabled, for instance, the identification, arrest and resulting conviction by the Lyon criminal Court of a man who stole a truckful of goods in a warehouse in the Lyon suburbs.[6] This case raised a lot of interesting issues. The defendant's attorney claimed that his client was used as a "guinea pig" for facial recognition[7] and he unsuccessfully challenged the use of the technology which helped identify his client. Indeed, in this case the Lyon criminal Court accepted the arguments of the prosecutor and the law enforcement authorities, that facial recognition was solely used to support the investigation and did not constitute "evidence" as such.

In 2012 already, the French branch of the NGO, the "Ligue des droits de l'Homme" was one of the first to challenge, before the Conseil d'Etat, the lawfulness of the decree authorising the use of facial recognition in relation to the TAJ system. The highest French administrative Court then confirmed the lawfulness and validity of the 2012 decree authorising the TAJ. It concluded that "The procedures for collecting, consulting and processing such data, under the conditions defined by the contested decree, are such as to guarantee the effectiveness of the establishment of offences that are against the criminal law, the gathering of evidence of such offences and the search for their perpetrators; that it follows that the collection of digitised photographs of persons implicated or under investigation or inquiry for the search for the causes of death or disappearance is, taking into account the restrictions and precautions to which this processing is subject, adequate, relevant and not excessive in relation to the legitimate purposes".[8]

Despite this initial ruling which validated the decree introducing the TAJ, La Quadrature du Net filed a new complaint in 2020

[3] In particular, article R 40-26 of the code of criminal procedure reads as follows: "The following categories of personal data and information may be recorded in this processing operation 1° Concerning the accused persons : a) Natural persons: […] - a photograph with technical features that allows a facial recognition device to be applied to it (facial photograph) […] 3° Concerning persons who are the subject of an investigation or enquiry into the causes of death or disappearance: […] - Photographs with technical characteristics that allow a facial recognition device to be applied to it (facial photographs of missing persons and unidentified bodies".

[4] *Summary report of the project 'Towards the European Level Exchange of Facial Images*, *Telefi Project*, Version 1.0, January 2021, 70, available at: https://www.telefi-project.eu/sites/default/files/TELEFI SummaryReport.pdf.

[5] *Ibidem*, 72.

[6] R. Gardette, *Un logiciel de reconnaissance faciale utilisé lors d'un procès à Lyon fait débat*, France 3 régions, 18 September 2019, available at: https://france3-regions.francetvinfo.fr/auvergne-rhone-alpes/rhone/lyon/logiciel-reconnaissance-faciale-utilise-lors-proces-lyon-1724157.html.

[7] D. Lepetitgaland, *Première en France: à Lyon, la reconnaissance faciale le désigne, il est condamné*, *Le Progrès*, 1 November 2019, available at: www.leprogres.fr/rhone-69/2019/11/01/la-reconnaissance-faciale-le-designe-il-est-condamne.

[8] Conseil d'État, 10ème / 9ème SSR, 11 April 2014, 360759, available at: www.legifrance.gouv.fr/ceta/id/CETATEXT000028842861.

requesting that the Conseil d'État invalidate the provisions in the code of Criminal Procedure which expressly concern the option of resorting to facial recognition technology in combination with the TAJ database. LQDN's request therefore specifically concerned the use of facial recognition and not the TAJ system as a whole. It was also unprecedented in that it was based on the claim that the relevant provisions of the French code of Criminal Procedure were contrary to Article 10 of the LED, which was adopted in 2016 and only entered into force in 2018. This complaint led to the decision issued on 26 April 2022 by the Conseil d'Etat.

2. *The LQDN's claims*

As mentioned above, LQDN is a fierce opponent of facial recognition technology. On 12 November 2019 LQDN issued "a request for the repeal of paragraphs 16 and 59 of Article R. 40-26 of the Code of Criminal Procedure, which describes the TAJ system" to the Prime Minister, Minister of the Interior and the Minister of Justice.[9]

Since the Government did not repeal the contested provisions, LQDN referred their tacit refusal to invalidate the provisions to the Conseil d'Etat. LQDN challenged the idea that article R 40-26 of the code of criminal procedure complies with article 10 of the Law enforcement directive, which provides that "[p]rocessing of […] biometric data for the purpose of uniquely identifying a natural person […] shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject".[10]

It is important to note from the outset that that the French version of the LED translates the "strict necessity" criterion as "necessité absolue", which translates back as "*absolute* necessity". This translation seems to increase the significance of the necessity criterion.

LQDN claimed that "there is no 'absolute necessity' that can legally justify such measures in this case".[11] In its letter of response to LQDN sent on February 12 , 2020, the Minister of Justice stated that "the facial recognition device constitutes a technical aid to the investigator's reconciliation of information obtained in the course of the investigations carried out".[12] LQDN seems to consider that since the Government describes facial recognition as a mere "technical aid" to police officers, this tool is not "absolutely necessary" to carry out the investigation and the image matching used to identify suspects. On this topic LQDN stated that "[t]he role of 'technical assistance', is in essence not in accordance with the 'absolute necessity' criterion. In other words, recognising the mere 'usefulness' of the device demonstrates the absence of 'necessity' and, a fortiori, the absence of the 'absolute necessity' required to legally justify such a device".[13] LQDN therefore considered that something which is merely viewed as a form of assistance cannot at the same time be viewed as indispensable. However, the Conseil d'Etat did not agree.

3. *The Conseil d'Etat's interpretation of the strict necessity requirement*

Even though the French version of Article 10 of the LED seems to propose an interpretation of the "strict necessity" requirement that is even more rigid than that used in the English version, the Conseil d'Etat did not accept the LQDN interpretation. On the contrary, it concluded that: "[i]n view of the number of defendants registered in this processing, which amounts to several million, it is materially impossible for the competent officers to carry out such a comparison manually, and moreover with the same degree of reliability as that offered by a correctly parameterised facial recognition algorithm. However, such an identification based on a person's face and the comparison with the data recorded in the [TAJ] may prove to be absolutely necessary for the search for the perpetrators of offences and for the prevention

[9] See Conseil d'Etat, Section du contentieux, requête, 2 August 2020, available at: www.laquadrature.net/wp-content/uploads/sites/8/2020/08/LQDN-REQ-TAJ-02082020.pdf.

[10] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[11] See Conseil d'Etat, Section du contentieux, requête, 2 August 2020, 6., available at: www.laquadrature.net/wp-content/uploads/sites/8/2020/08/LQDN-REQ-TAJ-02082020.pdf.

[12] *Ibidem*.

[13] *Ibidem*.

of breaches of public order, both of which are necessary to safeguard rights and principles of constitutional value. Consequently, the recording of the data at issue in this processing operation meets the condition of absolute necessity laid down by the above-mentioned provisions".[14]

In other words, as regards the vast number of individuals included in the TAJ system, the facial recognition software is absolutely necessary for police officers to be able to effectively compare images in order to identify suspects and support criminal investigations.

This rationale did not convince LQDN, which characterised the Conseil d'Etat's reasoning as "circular".[15] LQDN questioned use of the TAJ precisely because it considered this database to be "a mass surveillance tool", which is so massive that it necessitates the use of facial recognition in order for it to work. Therefore, according to LQDN, the Conseil d'Etat reinforces the logic of surveillance more than it diminishes it. LQDN stated to prove this point that "[o]ne mass surveillance (generalised data collection) requires another mass surveillance (generalised facial recognition)".[16]

However, the Conseil d'Etat's reasoning is not really surprising since it had already had the opportunity to interpret the strict (or "absolute" in French) necessity requirement in relation to article 88 of the amended law of 6 January 1978 - which basically transposes article 10 of the LED into French law - in a decision dated 4 January 2021.[17] The Conseil d'Etat had to rule on the lawfulness of a decree which modified certain provisions related to the "Prévention des atteintes à la sécurité publique" ("prevention of public security breaches") database, which is another police database.[18] The abovementioned decree empowered the police to collect and store data containing people's political opinions, religious beliefs, and many other sensitive data, for specific purposes such as the protection of State security.[19] On that occasion, the Conseil d'Etat stated the following: "Article R. 236-12 of the Internal Security Code, as drafted by Article 2 of the contested decree, provides that data may only be recorded insofar as they are strictly necessary for the purposes of the processing. It specifies that only activities 'likely to undermine public security or State security' may give rise to the recording of data on public activities or activities within groups or legal entities or activities on social networks, which prohibits, in particular, the recording of persons in the processing operation based on mere trade union membership. It should also be noted, as the administration argued before the interim relief judge, that the possibility of recording data relating to activities likely to undermine public security on the networks can only come from data collected individually and manually. […] In these circumstances, it does not appear, in the light of the investigation, that the processing of these data does not meet an absolute necessity with regard to the purposes of preventing risks to public security and is not accompanied by appropriate guarantees".[20]

In conclusion, the Conseil d'Etat considered that the processing of sensitive data was compliant with the 'absolute necessity' requirement as laid down by article 88 of the law of 6 January 1978 be it for protecting State security or to carry out investigations. It remains to be seen whether the Conseil d'Etat would have been able to criticise article R 40-26 of the code of criminal procedure on other grounds, such as the proportionality requirement.

4. *Ex-post biometric identification and the proportionality requirement*

The proportionality principle complements the necessity principle, since for a data processing operation to be deemed lawful, it must be strictly necessary and proportionate to

[14] Conseil d'État, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

[15] *Le Conseil d'Etat sauve la reconnaissance faciale du fichier TAJ*, *La quadrature du Net*, 3 May 2022, available at: www.laquadrature.net/2022/05/03/le-conseil-detat-sauve-la-reconnaissance-faciale-du-fichier-taj.

[16] *Ibidem.*

[17] See Conseil d'État, Décision No. 447970, 4 January 2021, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-01-04/447970.

[18] See Decree No. 1511, 2 December 2020, amending the provisions of the *code de la sécurité intérieure* relating to the processing of personal data known as *Prévention des atteintes à la sécurité publique*, available at: www.legifrance.gouv.fr/jorf/id/JORFTEXT000042607323.

[19] *Ibidem.*

[20] Conseil d'État, Décision No. 447970, 4 January 2021, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-01-04/447970.

the aim pursued by the data controller. Consequently, the Conseil d'Etat also assessed the proportionality of the use of facial recognition for face matching purposes by the police in relation to the TAJ system consultation. The Conseil d'Etat considered that use of the system was sufficiently regulated and that it was proportionate as regards the aim pursued, i.e, crime prevention, investigation and repression.

In particular, the Conseil d'Etat considered that: "Facial recognition devices may only be used by the competent services in cases of absolute necessity, assessed solely in the light of the purposes of the processing operation, where there is doubt as to the identity of a person whose identification is required. This identification, assisted by this system, is the responsibility of the officials themselves. The regulatory provisions at issue, which govern only the use of [TAJ] are not intended to define the conditions for collecting images of people in public spaces or posted on social networks, nor to authorise the systematic or large-scale comparison of such images with the biometric templates stored in this processing. […] It follows that the contested processing operation contains appropriate safeguards for the rights and freedoms of the data subjects and does not, contrary to what is claimed, establish a 'disproportionate mechanism'".[21]

It is worth noting that the Conseil d'Etat assessed the proportionality of this specific use of facial recognition for criminal investigations by comparing it with other ways in which facial recognition is used by law enforcement agencies. The Conseil d'Etat therefore seemed to be making a distinction between using it in this specific way and using facial recognition in "real-time" when deploying systems in public places that match all bystanders' faces with the faces of people who appear in a particular watchlist. [22] The Conseil d'Etat stated in this respect that "[t]he regulatory provisions at issue, which govern only the use of the [TAJ], are not intended […] to authorise the systematic or large-scale comparison of such images with the biometric templates recorded in this processing".[23]

Similarly, the Conseil d'Etat considered that the provisions that concern the TAJ database "are not intended to define the conditions for collecting images of people in public spaces or posted on social networks".[24] Such systems may encompass systems such as Clearview AI software which has been deemed unlawful by many Data Protection Authorities (DPA) across Europe.[25]

With these considerations taken into account, the Conseil d'Etat concludes that "the contested processing operation contains appropriate safeguards for the rights and freedoms of the data subjects and does not, contrary to what is claimed, establish a 'disproportionate mechanism'".[26]

The Judges' reasoning suggests that the purpose of Article R 40-26 of the Code of Criminal procedure is not to authorise large-scale face matching devices or to authorise facial recognition systems such as Clearview AI, which provides law enforcement agencies with a database of images of individuals taken from the open web and notably from social networks. The Conseil d'Etat seems to acknowledge that the TAJ system is provided for by legal provisions and is less intrusive than other approaches, such as the automated processing of images from social media or the large-scale deployment of facial recognition devices.

5. *The Conseil d'Etat's decision from a comparative perspective*

The Conseil d'Etat's decision comes at a time of great debates in Europe about the use of facial recognition technologies in general and the specific way in which these

[21] Conseil d'État, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

[22] We categorise this kind of systems as "Large-scale face matching use-cases", see T. Christakis, K. Bannelier, C. Castelluccia and D. Le Métayer, *Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 2: Classification*, Report of the AI-Regulation Chair (AI-Regulation. Com), MIAI, May 2022.

[23] Conseil d'Etat, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

[24] *Ibidem*.

[25] See for instance, ICO, *Enforcement Powers of the Information Commissioner: Monetary Penalty Notice*, available at: https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/, or CNIL, Décision MED-2021-134 du 26 novembre 2021, available at: www.legifrance.gouv.fr/cnil/id/CNILTEXT000044499030, last accessed on 7 April 2022.

[26] Conseil d'Etat, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

technologies are used by law enforcement agencies in particular. The Conseil d'Etat's decision should therefore also be interpreted in the context of these debates. We would like to make four series of observations in this respect.

1) First, it should be noted that law enforcement authorities in Europe are increasingly using new technologies in general and facial recognition in particular in order to identify suspects. According to the TELEFI project study, as of the date of December 2020 facial recognition had been implemented in a similar way to the French TAJ system in 10 other EU Member States (Austria, Finland, Germany, Greece, Hungary, Italy, Latvia, Lithuania, The Netherlands and Slovenia), in the UK and by Europol and Interpol. 7 EU Member States (Croatia, Cyprus, Czech Republic, Estonia, Romania, Spain and Sweden) had reached the stage of preparing for implementation, and they were expected to start using the technology within one to two years.[27] While the legal landscape concerning the use of facial images in criminal investigations varies significantly from one EU country to another, all of these countries are subject to the "strict necessity" and proportionality requirements of the LED. From this point of view the decision of the Conseil d'Etat could reinforce the argument about using facial recognition to support criminal investigations in Europe.

2) It should also be noted that the Conseil d'Etat's decision is not the first time that the "strict necessity" and proportionality of the use of facial recognition to support criminal investigations has been assessed in Europe. As a matter of fact, a few DPAs and Courts in EU Member States and the UK have already had the opportunity to adopt a position on this issue.

A decision of particular relevance to this issue was issued by the 'Garante per la protezione dei dati personali', the Italian DPA. As a matter of fact, the Italian police use a system called "SARI-Enterprise" which basically enables police officers to match the photograph of a suspect with the AFIS-SSA database. In this respect the system is very similar to the French TAJ system. When analysing the lawfulness of such a system, the Italian DPA stated that it was "a mere assistance to human action".[28]

In other words, both the "Conseil d'Etat" and the "Garante" considered that given that the facial recognition systems were used as a mere assistance to police work, the LED's "strict necessity" requirement would be met.

3) The third series of observations concerns the relationship between the issue being considered by the Conseil d'Etat and the legislative work currently being undertaken by the EU Institutions regarding the EU Commission's proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act).[29] Article 5 of the draft regulation includes, in the list of prohibited AI practices, "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement"[30] except when these systems fulfil certain specific, listed purposes. However, these "Real-Time biometric identification systems" do not cover systems such as the TAJ since the latter is not intended to be deployed in real-time. The AI Act proposal does not therefore prohibit biometric ex-post identification of individuals for criminal investigation purposes. Nonetheless, such systems will be submitted to the pre-market requirements imposed by the draft AI Act.[31]

4) A final series of observations concerns the relationship between the Conseil d'Etat's decision dated 26 April 2022 and the first version of the Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted by the European

[27] See the *Summary report of the project 'Towards the European Level Exchange of Facial Images*, *Telefi Project*, Version 1.0, January 2021, 10, available at: www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf.

[28] Garante per la Protezione dei Dati Personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 July 2018, available at: www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9040256.

[29] 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, com/2021/206 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[30] *Ibidem*.

[31] See T. Christakis, *Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021*, 27 May 2021, available at: https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021.

Data Protection Board on 12 May 2022 and consequently submitted for public consultation.[32] According to the EDPB, "such tools should be used in strict compliance with the applicable legal framework and only in cases where they satisfy the requirements of necessity and proportionality […] while modern technologies may be part of the solution, they are by no means a 'silver bullet'".[33]

The EDPB specifies the conditions under which a facial recognition system used for investigation purposes may be considered lawful. In particular, the EDPB states that "[t]he national law must be sufficiently clear in its terms to give data subjects an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such measures".[34] Furthermore, as regards the necessity requirement, the EDPB considers that "[p]rocessing can only be regarded as 'strictly necessary' if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary. […] This requirement should be interpreted as being indispensable".[35] As mentioned previously, LQDN claimed that the reasoning of the Conseil d'Etat was flawed because something that is perceived as providing mere assistance should not, in their opinion, be considered indispensable.

In view of the above, it remains to be seen whether NGOs such as LQDN will make use of these guidelines, and especially the specifications proposed by the EDPB for there to be law of sufficient "quality" and "special safeguards", in order to challenge, in future, the facial recognition provisions of the French Code of Criminal Procedure.

6. *Conclusion*

The Conseil d'Etat's decision reaffirms the validity of article R 40-26 of the code of criminal procedure, which expressly provides for the option to resort to facial recognition in criminal investigations. The Conseil d'Etat claims that using facial recognition in such a way is necessary when the amount of data available to the police is taken into account, and that it is proportionate to the aim pursued. This decision is part of a wider issue in Europe, where facial recognition for investigative purposes has been under the spotlight. Indeed, States are currently thinking about which facial recognition techniques should be prohibited and what facial recognition uses should be authorised, assuming that adequate safeguards are put in place. The view of the Conseil d'Etat, together with that of the Italian DPA, tends to suggest that States consider that deploying facial recognition for ex-post individual identification purposes is necessary and proportionate to the aim pursued, which is to repress crime. The EDPB and the draft AI Act also align in terms of allowing such deployments if there is an appropriate national legal framework providing proper safeguards.

[32] European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 1.0, 12 May 2022, available at: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.
[33] *Ibid*, 26.
[34] *Ibid*, 18.
[35] *Ibid*, 19.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 167-172
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 15

*The Digital Administration of Foreigners in France**

Quentin Ricordel
(PhD in public law at the University of Limoges)

French Council of State, 3 June 2022, La Cimade et autres, n. 452798

French Council of State, 3 June 2022, La Cimade, n. 461694

In two decisions of 3 June 2022, the French Council of State ruled on the legality of the digital administration of foreigners in France. While it largely accepted the possibility for the administration to propose, and even impose, the use of a teleservice, it attached several guarantees to this option.

ABSTRACT This case note analyses the decisions La Cimade ruled by the French Council of State. It is a question of knowing how far the reception of foreigners can be dematerialized and to replace these solutions in the perspective of the evolution of user's rights faced with the digitisation of the administration.

1. *Introduction*

Like others, foreigners are not immune to the phenomenon of digitisation of the administration. The dematerialization of procedures quickly appeared to the public authorities as the best way to put an end to the infringements of fundamental rights observed in the context of the physical reception of foreigners in the administrations.

Numerous reports[1] had noted the serious consequences of the administration's inability to properly organize the reception of foreigners, in particular the endless queues outside, with no guarantee of being able to access the counter. The Government has therefore sought to resolve these difficulties by gradually digitising reception procedures and developing a teleservice for foreigners. Notably, it has dematerialized the booking of appointments and the submission of a number of required documents. The decree of 24 March 2021[2] constitutes a new stage in this process by creating a dedicated online service for submitting applications for certain residence permits.

This text was referred to the Council of State for several reasons. On the one hand, an association for the defense of the rights of foreigners, La Cimade, has asked the administrations to provide alternative methods for receiving users. She then contested the implicit refusals which were opposed to her before the administrative courts. Two of them seized the Council of State with a request for an opinion on the basis of article L. 113-1 of the Code de justice administrative, which allows a court to transmit to the supreme administrative judge a "new question of law, presenting a serious difficulty and arising in many disputes". On the other hand, the same association directly attacked the decree of 24 March 2021 which instituted teleservice and the decree of 27 April 2021 which specified certain terms and conditions.

The questions put to the administrative judge were therefore relatively numerous, but they can be summarized as to what extent the administration can require foreigners to carry out their formalities by means of a dematerialized procedure.

In an opinion[3] and a decision[4] *La Cimade*, returned in section – the second most solemn

* Article submitted to double-blind peer review.

[1] In particular: General Administration Inspectorate, *Reception of foreign nationals by prefectures and sub-prefectures*, 2014, 31, in www.interieur.gouv.fr; Defender of Rights, *The fundamental rights of foreigners in France,* 2016, 44, in www.defenseurdesdroits.fr; Defender of rights, *Dematerialization and inequalities of access to public service*, 2019, 21, in www.defenseurdesdroits.fr; Council of State, *Twenty proposals to simplify litigation for foreigners in the interest of all*, 2020, 54, in www.conseil-etat.fr.

[2] Decree n. 313, 24 March 2021, relating to the establishment of a teleservice for submitting applications for residence permits.

[3] Council of State, 3 June 2022, *La Cimade*, n. 461694.

[4] Council of State, 3 June 2022, *La Cimade et autres*, n. 452798.

formation –, the Council of State provided important details on the legal regime of the digitisation of the public service for foreigners. Although he widely accepted the principle (2.), it accompanied this approach with a certain number of guarantees which, not fulfilled by the texts, led to their partial cancellation (3.).

2. *The consecration of the digitisation of the administration of foreigners*

The development of the digitisation of administrative activities requires the removal of various obstacles. If it is necessary to build a flexible framework allowing the administration to easily dematerialize its procedures (2.1.), the generalization of the process sometimes implies imposing it, which raises other difficulties (2.2.).

2.1. *The right to propose the use of a teleservice*

In general, users have the right to contact the administration electronically. This possibility was granted to them by an ordinance of 8 December 2005,[5] since codified in articles L. 112-8 and following of the Code des relations entre le public et l'administration (CRPA). This right is reflected into an obligation for the administration to put in place the digital tools suitable for allowing citizens to address it electronically and by the possibility of creating teleservices for this purpose.[6]

The difficulty is that several procedures involve a personal presentation of the foreigner.[7] This requirement directly conflicts with the obligation for the administration to set up a digital procedure and logically prevents users from requesting dematerialization.[8] On the other hand, it does not necessarily exclude the possibility of creating a teleservice for carrying out the steps prior to the personal presentation of the foreigner, such as making an appointment. The basis for such digitisation was not obvious since it cannot be sought in the right of citizens to seize the administration by electronic means, since this right is precisely excluded. The Council of State has therefore chosen to link this option to the organisational power of the head of department[9] "Unless there are special provisions, the prefects can create teleservices for the accomplishment of all or part of the administrative procedures for users".[10] The rapporteur public – a judge who publicly and independently expresses his or her opinion on the issues to be decided in the applications and on the solutions they call for – also recalled the relevance of dematerialization in this case, as "it is a priori quite paradoxical to have to come and queue in front of the prefecture to obtain an appointment, that is to say in the sole purpose of being able to come back a few days or weeks later".[11]

The decree of 24 March 2021 relaxed the requirement of the personal presentation of the applicant by reducing it to certain specific requests. Since its entry into force, the situation has therefore been as follows: either the foreigner's request is part of a procedure which requires him to physically present himself before the administration, in which case digitisation is only possible for certain stages of the procedure, either his approach is not affected by this obligation, in which case the administration is free to provide for an entirely dematerialized system, or even to impose it.

2.2. *The right to impose the use of a teleservice*

The main grievance against the digitisation process concerns the possibility of forcing foreigners to use digital services to contact the administration. It is true that the Council of State had not really pronounced on the question.

A first decision could have been interpreted as preventing the administration from forcing users to contact it digitally.[12] It was a question

[5] Ordinance n. 1516, 8 December 2005, relating to electronic exchanges between users and administrative authorities and between administrative authorities.
[6] Decree n. 685, 27 May 2016, authorizing teleservices aimed at implementing the right of users to contact the administration electronically.
[7] Former article R. 311-1 of the Code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA).
[8] Article L. 112-10 of the CRPA; Decree n. 1423, 5 November 2015, relating to exceptions to the application of the right of users to contact the administration electronically.
[9] Council of State, 7 February 1936, *Sieur Jamart,* n. 43321, in *Les grands arrêts du droit administratif*, XXIII ed., Paris, Dalloz, 2021, 293.
[10] Council of State, section, opinion, 3 June 2022, *La Cimade*, n. 461694.
[11] L. Domingo, *Téléservice public : institution et fonctionnement - Le cas des demandes de titre de séjour des étrangers*, in *Revue française de droit administratif*, 2022, 761.
[12] Council of State, 27 November 2019, *La Cimade et*

of deciding on the scope of article L. 112-9 of the CRPA, which affirms that "when it has set up a teleservice reserved for the performance of certain administrative procedures, an administration is regularly contacted electronically only through the use of this teleservice". La Cimade had challenged the Prime Minister's refusal to modify the implementing decree for this text.[13] She criticized him for not having specified the optional nature of the digital referral to the administration. The administrative judge considered that the purpose of the contested decree was not to make the use of a teleservice compulsory in general, but only to allow the administration to impose its use on users wishing to enter into contact by digital means. This therefore left open the possibility of seizing the administration by the traditional route, by post or by physically going to its counter.

This decision should not be interpreted as conditioning the legality of a teleservice procedure on its optional nature. The decision is limited to considering that the decree which was challenged did not have the scope attributed to it by the applicants, which does not mean that it would have been illegal if it had had it. The plea was ineffective, that is to say incapable of influencing the legality of the decision, which does not prejudge its merits. The decision is therefore not, as was thought, "a brake on the digital transformation of the public service",[14] but a simple clarification of the scope of one rule, which does not prevent another rule from imposing the dematerialization of a procedure.

Freed from a misinterpretation of its previous case law, the Council of State provides a nuanced response to the question of the mandatory nature of teleservices. Firstly, although the prefect may, as part of his power to organise the service, propose a teleservice to users, he does not derive the power to impose it on them. This means that before the decree of 24 March 2021 came into force and, since then, for cases not covered by it, the teleservices set up in the prefectures are optional and do not prevent foreigners from contacting the administration by more traditional means.

On the other hand, the prefect can impose a teleservice on users who wish to contact him electronically. This point is not directly addressed in the decision or the commented opinion, but it follows from certain solutions they provide. Since the right of citizens to contact the administration electronically authorizes the public authorities to impose the use of a teleservice for this purpose, it seems obvious that they can do so when the user can't assert any rights, as is the case for foreigners. In other words, as long as the administration is not required to propose a means of contacting it digitally, it must remain free, if it does so, to organise the arrangements for this contact as it wishes, including by imposing the use of a teleservice.

Above all, the administrative judge considers that there is no principle that requires citizens to be free to choose their method of contact with the administration. This position should not come as a surprise, as the Council of State had adopted an identical solution with regard to the procedures for registering applications before the courts and ruled that "no principle of administrative litigation procedure, nor any legislative provision, requires that applicants be given the option of bringing an application directly before an administrative court".[15] It was at the time of the obligation to address his request by mail rather than directly to the registry, the reasoning is perfectly transposable to digitisation and indeed has not failed to be so.

It follows that by adopting a special text, the Government can impose on users the use of a teleservice in their procedures, "in particular to request the issuance of an authorization".[16] However, it is precisely the object of the contested decree to force the use of digital services. The decision therefore marks the possibility of a new impetus for the digitisation of public services by allowing, in principle, the elimination of all physical or epistolary contact between users and the administration. Naturally, such a possibility cannot be envisaged without being accompanied by a certain number of guarantees.

autres, n. 422516; note A. Sée, *Le recours aux téléservices ne peut être obligatoire*, in *Droit administratif*, n. 7, 2020, 49.

[13] Decree n. 685, 27 May 2016, authorizing teleservices aimed at implementing the right of users to contact the administration electronically.

[14] A. Sée, *Le recours aux téléservices ne peut être obligatoire*, 49.

[15] Council of State, 18 March 1988, *Association " France Terre d'Asile "*, n. 66807.

[16] Council of State, 3 June 2022, *La Cimade et autres*, n. 452798.

3. *The restriction of the digitisation of the administration of foreigners*

Administrative case law is permissive, but it offers citizens certain guarantees. On the one hand, it prevents the digitisation of the administration from resulting in the exclusion of certain categories of citizens (3.1.). On the other hand, it imposes on the administration a certain number of obligations to ensure that the digitisation of the public service does not lead to a reduction in the level of service offered to users (3.2.).

3.1. *The obligation to provide alternative means*

The decision oh 3 June 2022 specifies that "the regulatory power can only enact such an obligation on the condition of allowing users normal access to the public service and guaranteeing the persons concerned the effective exercise of their rights. It must consider the purpose of the service, the degree of complexity of the administrative procedures in question and their consequences for the interested parties, the characteristics of the digital tool implemented as well as those of the public concerned, in particular, the case where appropriate, of his difficulties in accessing online services or in their use".

This solution is consistent with the idea that users have the right to access the public service under normal conditions. The administrative case law on this issue is not the densest, but it shows some consistency. Already in 1911, the Council of State censured, under the angle of the fault, a post office which had closed during its opening hours.[17] As the rapporteur public pointed out, the principles of continuity of public service and equal treatment lead to the prohibition of unreasonable restrictions on access to public services. The administrative judge thus conditioned the adaptation of certain services on Saturdays, such as a post office[18] or a library,[19] to the absence of abnormal restrictions on user access.

More recently, the administrative judge has shown concern for preserving a certain level of accessibility to users. In a decision Commune de Saint-Méen-le-Grand of 1 October 2018, it ruled, with regard to the closure of a local treasury, that "the regulatory power could legally take into account, in particular, the criterion of the level of activity of the accounting posts that it planned to restructure, it had to combine it with other requirements, in particular the accessibility of public services and equal access for users to these services".[20] The decision is interesting in that it justifies the reduction in the level of activity of the service by the development of digitised procedures and ensures that, despite the elimination of the treasury, citizens do have access to a physical counter in a perimeter reasonable geography. As we can see, the Council of State's decision is the extension of well-established case law that it was very easy to transport to the field of digitisation of public services.

Moreover, the administrative judge had already ruled out the possibility for a university to organize a selection procedure based on the order of connection to a digital service – the Minitel – "in view of the conditions of telematics and computer equipment of the interested parties, the technical connection possibilities and the resulting differences in the conditions for routing their calls to the university's telematics server".[21] The opinion is very interesting in that it does not exclude in principle the use of a dematerialized process, nor even the obligation to use it, but surrounds this use with conditions which, when they are not met, require the administration to provide alternative methods. The decision of 3 June 2022 is a continuation of this solution.

It is interesting that an identical balance has been sought by the European Court of Human Rights, which, in a judgment of 9 June 2022, condemned France for having imposed disproportionately the use of digitisation for the referral judicial courts.[22] The reasoning followed by the Council of State is therefore part of a logic that is not unknown to European law, which should not come as a surprise.

Naturally, the point of balance between

[17] Council of State, 3 February 1911, *Anguet*, n. 34922.
[18] Council of State, 25 June 1969, *Vincent*, n. 69449; note R. Denoix de Saint-Marc, J.L. Dewost, *Chronique générale de jurisprudence administrative française*, in *Actualité juridique droit administratif*, 1969, 334.
[19] Council of State, 26 July 1985, *Association " Défense des intérêts des lecteurs de la Bibliothèque Nationale "*, n. 50132.
[20] Council of State, 1 October 2018, *Commune de Saint-Méen-le-Grand*, n. 404677.
[21] Council of State, 15 January 1997, *M. Gouzien*, n. 182777.
[22] European Court of Human Rights, 9 June 2022, *Xavier Lucas versus France*, n. 15567/20.

digitisation and the guarantee of access to the public service cannot be the same in all cases. From this point of view, the rapporteur public noted that foreigners, although they certainly do not constitute a homogeneous category, form a group which is more sensitive to changes in the public service, considering, notably an insufficient command of the language. This situation is reinforced by the complexity inherent in contemporary foreigner's law, which "has become a law for experts, [whereas] foreigners are not".[23] It follows that the administration must, on the one hand, provide support for foreigners who encounter difficulties in using the digital service offered and, on the other hand, provide a means of substitution when this support is not sufficient to guarantee them access to public service.

The first point did not present much difficulty in this case since the decree itself provided for support. Article R. 431-2 of the CESEDA, which results therefrom, provides that "persons who are not in a position to carry out the online filing of their application benefit from a welcome and support allowing them to complete this formality". This support takes the form of a call center as well as the creation, in the prefecture, of a reception point to help foreigners complete their formalities on the teleservice. Beyond the obvious shortcomings of this system – in particular the fact that the reception points are often only accessible by appointment, made on the internet – this guarantee, which is necessary, is sometimes insufficient.

There are indeed cases in which the digital tool does not meet the expectations of users because their situation is too specific to be processed automatically. The rapporteur public indicated, for example, that the teleservice in question did not manage changes of status, which are however common in foreigners law. By the way, administrative justice had already noted the shortcomings of this type of website.[24] Certainly, there are cases in which "digital interaction cannot completely replace human interaction".[25] In this situation, it is important that the administration provides, on a subsidiary basis, a means for foreigners to access the public service and to be able to register their request.

No means of substitution being provided for by the contested decree, the Council of State canceled it insofar as it did not provide for alternative methods of referral. This solution, which must be supported in that it makes it possible to promote the development of digital tools while preserving the very essence of public service, contributes to perfecting the legal regime for the dematerialization of public services, which case law had already begun to build.

3.2. *The obligation to maintain a certain level of service*

While they undoubtedly do not exhaust the question of the digitisation of the administration of foreigners, the decision and the commented opinion are also the culmination of a whole jurisprudential movement born of the recent development of a dispute over digitisation. Faced with the difficulties arising from the dematerialization of administrative procedures for foreigners, the administrative judge has sought to circumscribe the disadvantages.

The administrative judge has, for several years, frequently been seized of the refusal of appointments opposed to foreigners by the teleservice with which they are supposed to register. In a decision M. Bhiri of 10 June 2020,[26] the Council of State considered, about a foreigner who had unsuccessfully asked to be received, that it "is incumbent on the administrative authority, after having fixed an appointment, to receive him at the prefecture and, if his file is complete, to register his request, within a reasonable time". The conclusions of the rapporteur public let it be understood that the administration could not reasonably leave the foreigner without an answer for more than a month "access to public service, which itself conditions here access to rights, cannot be altered by referring the user to a faulty computer system".[27] The decision of the Council of State is even more demanding since it allows the foreigner to obtain an injunction from the judge if he testifies to several attempts "not having been

[23] L. Domingo, *Téléservice public : institution et fonctionnement - Le cas des demandes de titre de séjour des étrangers*, in *Revue française de droit administratif*, 2022, 761.
[24] Council of State, 18 February 2022, *Mme D.*, n. 455740.
[25] D. Charbonnel, *Une relecture des lois du service public*, PHD thesis, University of Limoges, Limoges, 2018, 474.
[26] Council of State, 10 June 2020, *M. Bhiri*, n. 435594.
[27] M. Le Corre, *Opinion on Council of State*, 10 June 2020, *M. Bhiri*, n. 435594, in www.conseil-etat.fr.

carried out in the same week".

Jurisprudence has also been confronted with the related problem of foreigners for whom an appointment is fixed, but at a date too distant for the renewal of their permit to take place before its expiry. From this point of view, the dematerialization of procedures takes the user away from the public service, but it also takes the administration away from the decision that is taken. The administrative judge considered that the decision to set an appointment for a foreigner on a specific date did not reveal the refusal to place him on an earlier date.[28] The rapporteur public considered that, since the decision had been taken by an algorithm, its scope could not exceed the scope of the foreigner's request.[29] In other words, the administration can take decisions digitally without having an exact awareness of their scope and without, what is more serious, having to assume the consequences from a legal point of view. Except in an emergency, it is therefore up to the foreigner who wishes to obtain an appointment at an early date to make a request to the administration, then to wait for the algorithm's response indicating a specific date, then to ask the administration to bring this appointment forward, then to contest the possible refusal before the judge. The digitisation of procedures is not always a guarantee of simplification.

[28] Council of State, 1 July 2020, *M. et Mme Labassi*, n. 436288; note G. Éveillard, *Le statut contentieux de la convocation des étrangers en préfecture en vue du dépôt d'une demande de titre de séjour*, in *Droit administratif*, n. 11, 2020, 44.

[29] G. Odinet, *Opinion on Council of State*, opinion, 1 July 2020, *M. et Mme Labassi*, n. 436288, in www.conseil-etat.fr.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 173-208
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 16

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

THE EUROPEAN DECLARATION ON DIGITAL RIGHTS AND PRINCIPLES

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on the establishment of a European Declaration on digital rights and principles – COM (2022) 27 final of 26 January 2022

The Commission has proposed a Declaration on digital rights and principles for a human-centred digital transformation.

A declaration on rights and principles that will guide digital transformation within EU has been proposed by the Commission to the European Parliament and the Council.

The declaration is part of widest framework of the "Digital Compass: the European Model for the Digital Decade", i.e. its vision of Europe's digital transformation by 2030, presented on 9 March 2021.

This programme is based on 4 nice points:

digitally empowered citizens and highly qualified digital professionals;

sustainable, secure and high-performance digital infrastructures;

digital transformation of enterprises,

digitisation of public services.

To this end, in September 2021 EU Commission introduced a solid governance framework to achieve the digital goals in the form of a Pathway to the Digital Decade, which recent draft declarations aim to complement.

This declaration also builds on previous initiatives provided by Council of the European Union, including the Tallinn Declaration on e-government, the Berlin Declaration on the digital society and value-based digital governance, and the Lisbon Declaration: "Digital Democracy with a purpose", all of which are about a digital transformation model that strengthens human dimension for digital ecosystem, within digital single market as its core.

The draft declaration on digital rights and principles aims to be a clear reference point for all on the kind of digital transformation that Europe promotes and defends. It will also provide guidance to policy makers and businesses regarding new technologies. The rights and freedoms enshrined in the EU legal framework and the European values expressed in the principles should be respected both online and offline. Once jointly approved, the declaration will also define the approach to digital transformation that the EU will promote worldwide.

The declaration is based on EU law, from the treaties to the Charter of Fundamental Rights, but also on the case law of the Court of Justice.

In particular, draft declaration covers fundamental rights and principles for digital transformation, such as putting people and their rights at its centre, supporting solidarity and inclusion, ensuring freedom of choice online, promoting participation in the digital public space, increasing people's security, autonomy and responsibility, and promoting the sustainability of the digital future.

These rights and principles should accompany EU citizens in their daily lives: high-speed and affordable digital connectivity everywhere and for everyone, well-equipped classrooms and teachers with the right digital skills, easy access to public services, a safe digital environment for children, disconnection after working hours, provision of easily understandable information on the environmental impact of our products, control over how personal data is used and with whom it is shared.

THE USE OF AI IN PUBLIC SERVICES IN EUROPE

European Commission, Report - AI Watch. European landscape on the use of Artificial Intelligence by the Public Sector, Joint Research Centre, 1 June 2022

Second landscaping study presenting the results of the mapping of the use of AI in public services in Europe.

This report is the result of a second study conducted by AI Watch, the knowledge service of European Commission to monitor develop-

ment, adoption and impact of artificial intelligence workings in Europe.

The introduction of the AI Act regulation is very important and valuable for framing cases of AI adoption also in the public sector.

In this direction, this report presents the results of mapping the use of AI in public services.

In particular, it is based on:

an analysis of the national AI strategies of European Member States focusing on how these strategies describe policy actions to address the development of AI in the public sector,

an inventory of AI use cases in the public sector to provide an overview of the state of AI implementation in Europe, and

in-depth case studies illustrating the crucial factors and consequences for responsible AI development and adoption.

These three pillars are confirmed in the structure of this report. Chapter 2 provides an overview of the status of research and policy of research and policies to provide the background and context that guides the research conducted in the report.

After this overview, the analysis continues along the three pillars. Chapter 3 presents the analysis of national strategies, highlighting how Member States (and Norway) intend to stimulate the use of AI within their public sector. Chapter 4 reports the results of the mapping exercise, in which 686 cases of AI use in the public sector were categorised and classified. To provide a more detailed view of some of the ways in which AI is developed and used within public sector, Chapter 5 contains a comparative analysis of 8 in-depth case studies that describe how governments have developed and integrated AI in the public sector. The idea behind this analysis is to collect and share practices that can support and inspire other public organizations in implementing AI. Given the current spread of AI in the public sector, sharing concrete practices is becoming extremely important. The 8 cases should be seen as the first step in this direction, to be complemented by further research.

Chapter 6 suggests some policy recommendations derived from the analysis, with a focus on the organisational level. The report concludes in Chapter 7 with the main findings and recommendations for future research activities.

The study shows that the use of AI by public administrations is growing. AI technologies could significantly improve the effectiveness and efficiency of public administrations. However, AI adoption remains uneven and barriers to AI adoption require significant considerations by policymakers. In particular, ensuring right balance of public and private sector expertise and capabilities, ensuring strong collaboration, and improving data governance and risk mitigation are among the main avenues to be pursued.

The report provides for a new and novel perspective, adding new insights to the existing tool of knowledge on the topic, especially moving from a more theoretical and anecdotal view of AI in the public sector to a more systematic analysis.

CONNECTIVITY FOR THE DIGITAL TRANSFORMATION

European Commission, Study on Investing in Local and Regional Gigabit Networks. Opportunities and challenges for market investors in the EU, Luxembourg, March 2022

The study on investing in Gigabit connectivity results in several suggestions on how to encourage private investment in digital infrastructure to reach the connectivity targets.

The study about investment in Gigabit connectivity results in several suggestions on how to encourage private investment in digital infrastructure to achieve connectivity goals.

Private investment is key to achieve connectivity targets by the deadline of Digital Decade 2030. By 2030, the goal is to connect all EU households with Gigabit connectivity and all populated areas with 5G. Making advanced high-speed connectivity widely available will also be key resource to support Digital Decade's goals on digital skills, digital technology for business and availability of key public services online.

In 2020, the EIB planned an investment to fil the gap for EUR 250 billion in EU for Gigabit and 5G deployment in time to meet the 2025 medium-term targets. Private investment will therefore be essential to achieve 2030 targets, potentially leveraged by European and national public funding and financial instruments.

THE EUROPEAN DATA FLOW MONITORING

European Commission, Study on Mapping Data Flows, L. Collini, L. Rabuel, M. Carlberg (eds), Luxembourg, October 2021

Monitoring data flows in Europe: new study by the European Commission.

The European Commission recently published a study mapping and estimating the vol-

ume of data flows to ensure adequate cloud infrastructures in 27 Member States and Iceland, Norway, Switzerland and the United Kingdom.

The 'Study on Mapping Data Flows' report provides for an overview of volume and types of incoming and outgoing cloud data flows by economic sector, location, company size and type of cloud services. Policy makers, business leaders and public administrations can use the study as a reference point in their decision-making process for future business agreements, industry decisions and cloud investments.

For this purpose, a new methodology was developed to quantify data flows: it is a robust, new and replicable economic methodology to identify, map, estimate, analyse and monitor data flows in a holistic, systematic and aggregated way for Europe.

The results highlight the following:

in 2020, the largest data flows came from the health sector;

Germany had largest volume of flows;

by 2030 there will be 15 times more data flows from European companies than in 2020.

The Commission also announced that a follow-up study was launched this year to assess the economic value of data flows within the EU (in addition to their volume) and with third countries such as the US and China.

Measuring data flows in Europe and the rest of the world is one of the key actions in the European data strategy.

Analysing, mapping, quantifying and monitoring data flows within and outside the EU in the area of cloud computing is crucial to support decision-making, industrial choices and investment decisions. It is even crucial for assessing the competitiveness of European digital economy based on analysis of current and future patterns of data flows, while monitoring data circulation against principle of free movement of non-personal data within EU economy.

PROHIBITION OF GENERAL AND INDISCRIMINATE RETENTION OF TRAFFIC AND LOCATION DATA RELATING TO ELECTRONIC COMMUNICATIONS

Court of Justice of the European Union (CJEU) (Grand Chamber), Judgment of 5 April 2022, Case C-140/20, *G.D. v The Commissioner of the Garda Síochána and Others* – Request for a preliminary ruling under Article 267 TFEU from the Supreme Court (Ireland), made by decision of 25 March 2020, received at the Court on 4 August 2016, in the proceedings

Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Confidentiality of the communications – Providers of electronic communications services – General and indiscriminate retention of traffic and location data – Access to data – Subsequent court supervision – Directive 2002/58/EC – Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Possibility for a national court to restrict the temporal effect of a declaration of the invalidity of national legislation that is incompatible with EU law – Excluded. The Court confirms that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime. The national court may not impose a temporal limitation on the effects of a declaration of invalidity of a national law that provides for such retention.

In recent years, Court has ruled in several judgments on the topic of retention of and access to personal data in electronic communications sector.

In particular, in two judgments decided by judgment in Grand Chamber on 6 October 2020, Case C-512/18, *La Quadrature du Net and Others*, the Court confirmed its case-law stemming from *Tele2 Sverige* judgment on disproportionate nature of generalized and undifferentiated retention of traffic and location data. It also provided clarifications, in particular, as to scope of powers granted by Directive 'on privacy and electronic communications' to Member States concerning the retention of such data for the purposes of safeguarding national security and combating crime.

In the present case, reference for a preliminary ruling was made by Irish Supreme Court in the context of civil proceedings brought by a person sentenced to life imprisonment for a murder committed in Ireland. The latter challenged the compatibility with EU law of certain provisions of national law on retention of data generated in the context of electronic communications. Under that law, traffic data and location data relating to telephone calls of accused had been retained by providers of electronic communications services and made accessible to the police authorities. Doubts expressed by referring Court related in particular to compatibility with 'directive on privacy and electronic communications', read in light of that Charter, of a generalised and undifferentiated retention regime for such data in connection with the fight against se-

rious crime.

In its judgment, delivered in Grand Chamber, the Court confirms, specifying its scope, case-law stemming from the judgment in *La Quadrature du Net and Others*, pointing out that the generalised and undifferentiated retention of traffic and location data relating to electronic communications is not authorized in order to the aim of combating crime and preventing serious threats to public security. It also confirms the case-law stemming from the *Prokuratuur* judgment (Conditions of access to data relating to electronic communications), in particular with regard to the obligation to ensure access by competent national authorities to such retained data subject to a preventive check carried out either by a Court or by an independent administrative authority, on a police officer.

In fact, Directive on privacy and electronic communications does not merely regulate access to such data by means of safeguards designed to prevent abuse, but lays down, in particular, the principle of prohibiting the storage of traffic and location data. The retention of such data therefore constitutes, on the one hand, a derogation from that prohibition of storage and, on the other hand, an interference with fundamental right to privacy and to protection of personal data, enshrined in Articles 7 and 8 of the Charter.

Although Directive on privacy and electronic communications permits Member States to restrict these rights and obligations for purposes, in particular, of fighting crime, such restrictions must nevertheless comply, in particular, with the principle of proportionality. This principle requires compliance not only with the requirements of appropriateness and necessity, but also with that of the proportionality of such measures in relation to the objective pursued.

In particular, the Court recalled, confirming its previous case-law, that EU law does not preclude legislative measures which provide, under the conditions listed in judgment:

- the targeted retention of traffic data and location data according to people categories concerned or by a geographical criterion;
- the generalized and undifferentiated retention of IP addresses attributed to the origin of a connection;
- generalized and undifferentiated retention of data relating to the civil identity of users of electronic communication media; and
- the quick freeze retention of traffic and location data held by such service providers.

OBLIGATION ON ONLINE CONTENT-SHARING SERVICE PROVIDERS TO REVIEW, PRIOR TO ITS DISSEMINATION TO THE PUBLIC, THE CONTENT THAT USERS WISH TO UPLOAD TO THEIR PLATFORMS

Court of Justice of the European Union (CJEU) (Grand Chamber), Judgment of 26 April 2022, Case C-401/19, *Republic of Poland v European Parliament and Council of the European Union* - Action for annulment under Article 263 TFEU, brought on 24 May 2019

The Court of Justice dismisses the action brought by Poland against Article 17 of the directive on copyright and related rights in the Digital Single Market.

Directive 2019/790 on Copyright and Related Rights in the Digital Single Market provided for a new specific liability mechanism for providers of online content-sharing services. Article 17 of that Directive establishes the principle that providers are directly liable when protected works and other subject-matter are illegally uploaded by users of their services. However, the providers concerned may be exempted from this liability. To that end, they are required, in particular, in accordance with provisions of that article, to conform an active control on contents uploaded by users, in order to prevent the putting online of protected material which the right holders do not wish to make accessible on those services.

Poland brought an action seeking, principally, the annulment of subpar. (b) and subpar. (c) of Article 17(4) of Directive 2019/790 and, in the alternative, repeal of entire rule. It states, in essence, that those provisions require providers to carry out prior surveillance, by means of automatic filtering tools, of all content that their users wish to put online, without without adequate data control and monitoring provisions.

Ruling for first time on the interpretation of Directive 2019/790, the Court dismissed the action brought by the Poland, holding that the obligation on providers laid down by that Directive, consisting in an automatic prior check on content put online by users, is accompanied by adequate safeguards to ensure respect for their right to freedom of expression and information and to strike a real fair balance between that right and the right to intellectual property.

The Court found that, in order to avoid being held liable when users upload infringing content onto their platforms for which providers do not have authorization by those entitled, such providers must demonstrate that they respect all conditions for exemption set out in Article

17(4)(a), (b) and (c) of Directive 2019/790, namely:

- that they have made every effort to obtain an authorisation (point (a));
- that they have acted immediately to bring about the cessation of actual infringements of copyright on their platforms after such infringements have occurred and have been brought to their attention in a sufficiently reasoned manner by rightholders (subparagraph (c)); and
- that they have, after receiving such a notification or when such rightholders have provided them with relevant and necessary information prior to occurrence of an infringement of copyright, in accordance with high standards of professional diligence in the industry, taken the utmost efforts to prevent such infringements from occurring or being repeated (subparagraphs (b) and (c)).

The latter obligations therefore *de facto* require such providers to carry out prior scrutiny of the content that users wish to upload onto their platforms, provided that they have received, from right holders, information or notifications referred to in Article 17(4)(b) and (c) of that Directive. To that end, providers are required to use automatic recognition and filtering tools. However, such prior monitoring and filtering is liable to restrict an important means of disseminating content online and thus to constitute a limitation of right to freedom of expression and information guaranteed by Article 11 of the Charter. Moreover, that restriction is attributable to EU legislator, as direct consequence of that specific liability regime. Therefore, the Court holds that that regime entails a limitation on the exercise of on the free speech regime and free expression and information of users concerned.

GDPR: CONSUMER PROTECTION ASSOCIATIONS MAY BRING REPRESENTATIVE ACTIONS AGAINST INFRINGEMENTS OF PERSONAL DATA PROTECTION

Court of Justice of the European Union (CJEU) (Third Chamber), Judgment of 28 April 2022, Case C-319/20, Meta Platforms Ireland Limited, formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. - Request for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 28 May 2020, received at the Court on 15 July 2020.

Such an action could be brought irrespective of the concrete infringement of the data protection right of a data subject and in the absence of a mandate to that effect.

The company Meta Platforms (Facebook) promotes the sale of advertising space under www.facebook.de. The facebook.de internet platform contains, in particular, an area known as the '*App-Zentrum*' (App Center) in which it offers free games provided by third parties available to users. When consulting this area, the user is shown the indication that the use of the application in question enables the games-providing company to obtain an amount of personal data and authorises it to publish data on behalf of that user, such as his score and other relevant information.

The Federal Union (FU), a body empowered to bring actions under Article 4 of Injunctions Act, considered that indications provided by the games in question in App Center could be unfair, in particular legally speaking and for conditions applying to obtaining of valid user consent under provisions governing data protection. Furthermore, according to mentioned FU, there is one indication that penalizes users beyond measure. For these reasons, the FU brought an action for an injunction against Meta Platforms before the *Landgericht Berlin* (Berlin District Court, Germany), based on section 3a of the Law on regulation in the area of fair competition. That action was brought irrespective of concrete infringement of a data subject's right to data protection and in the absence of a warrant given by the same person.

The *Landgericht Berlin* (Berlin Regional Court) found against Meta Platforms. Meta Platforms appealed before the *Kammergericht Berlin* (Higher Regional Court, Berlin, Germany), but the action was dismissed. Meta Platforms then brought another appeal before the *Bundesgerichtshof* (Federal Court of Justice, Germany) against the rejection of the previous appeal.

The *Bundesgerichtshof*, referring Court, considered that action of Federal Union is well founded; however, it has doubts as to admissibility of its action. Therefore, he made a reference to the Court of Justice for a preliminary ruling, submitting the following question:

'Do the rules in Chapter VIII, in particular in Article 80(1) and (2) and Article 84(1), of Regulation (EU) 2016/679 preclude national rules which alongside the powers of intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the options for legal redress for data sub-

jects empower, on the one hand, competitors and, on the other, associations, entities and chambers entitled under national law, to bring proceedings for breaches of Regulation (EU) 2016/679, independently of the violation of rights of individual data subjects and without being mandated to do so by a data subject, against the infringer before the Civil Courts on the basis of prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions?'

In its judgment, the Court of Justice held that Article 80(2) of General Data Protection Regulation does not preclude in absolute terms a consumer protection association from being able to bring legal proceedings, in absence of a mandate granted to it for that purpose and independently of infringement of same specific rights of data subjects, against person allegedly liable for an infringement of laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of use of invalid general terms and conditions. Such an action is possible where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that Regulation.

Indeed, on the one hand, bringing of a representative action does not require a prior individual identification, by entity in question, of person specifically affected by a data processing allegedly contrary to the provisions of GDPR.

On the other hand, the bringing of such an action does not require the existence of a specific breach of the rights which a person enjoys under the GDPR. In order to recognise that an entity has standing to bring proceedings, it is sufficient to claim that the data processing concerned is liable to affect the rights which identified or identifiable natural persons derive from that regulation, without it being necessary to prove actual harm suffered by the data subject, in a given situation, by the infringement of his or her rights.

BELGIUM

edited by
Elise DEGRAVE, Professor at University of Namur. Director of investigation of 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
Pierre-Olivier PIELAET, teaching assistant at University of Namur, researcher at NADI-CRIDS and lawyer at Walloon Brabant Bar

DATA PROCESSING RELATED TO COVID 19 EPIDEMIC CRISIS

Court of First Instance of Namur, order 22/3/C of 30 November 2021

An interim action was filed against the Walloon Region for time extension of the framework imposing use of the Covid Safe ticket (i.e. a vaccination, test and recovery pass used to condition access to events and facilities during the pandemic) on the territory of Wallonia.

In Belgium, access to events and facilities during the pandemic was conditioned by presentation of a vaccination, test or recovery pass named "Covid Safe Ticket" (hereafter "CST"). Under CST legal framework, Belgium federated entities were allowed to impose the use CST to different events and facilities (e.g. restaurants and sport activities) through adoption of legal texts. As explained in the previous report, a judgment of the Liege Court of Appeal of 07 January 2022 confirmed the CST *prima facie* proportionality on the Wallonia territory in a context where the contamination rate was high. On 15 January 2022, Walloon Region modified its Decree to extend use of the CST until 16 April 2022. In this dispute, the claimants filed a new interim action against, among others, this Decree due to the apparition of new Omicron variant of COVID-19 virus. After recalling that use of CST was contrary to several fundamental rights including privacy, Court noticed that recent scientific data highlighted limited effects of vaccines against virus propagation. Furthermore, data showed a reduction of patients in intensive care. Hence, Region was not anymore able to establish proportionality and necessity of the measure regarding part of its objectives (i.e. reducing COVID-19 propagation and occupation in intensive care). Court decided that, based on epidemic data decision to extent duration of CST does not constitutes a *prima facie* fault of the Region. However, the Court also found that, at the time of the order, not ending or adapting the rules constitutes a *prima facie* fault. Therefore, the Court ordered the Region to take all appropriate steps end this harmful situation. The Court also imposed a penalty payment of 2500 euros per day.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 47/2022 of 4 April 2022

The BDPA ruled on the compliance with GDPR of passenger's temperature checks in a Belgian airport during COVID-19 epidemic crisis.

In this case, Inspection service of BDPA decided to start an investigation due to use of thermal cameras by the defendant (i.e. Brussels South Charleroi Airport) to avoid spread of COVID-19. In practice, defendant used thermal cameras for temperature checks of passengers. Their temperature was checked by thermal cameras. Where the temperature was above 38°C passengers were redirected to infirmary for another check with a thermometer. In case where temperature was confirmed passengers were orally questioned by emergency services. In such cases passengers were not admitted in flight terminals if flight operators refused on board access. According to the defendant, the data processing by means of thermal cameras was necessary for reasons of public interest in the area of public health under national law (Article 9.1.i) GDPR). The BDPA however ruled that the processing was unlawful among others for the following reasons. The first profile was related to the protocol adopted by national Transport Authority under a Ministerial Decree enshrining urgent measures during the epidemic crisis. As highlighted by State Council such protocols were not legally binding in Belgium law. Hence, it cannot constitute a sufficient legal basis. Second the processing cannot be considered as necessary since it was mentioned in the protocol temperature check of passengers was not recommended by EU Aviation Safety Agency. Authority also detected a violation of transparency principle as none of the various information sources of the defense mentioned use of thermal cameras. It stressed that even if this information was relayed in press media, data controller is not relieved of transparency duties. Additionally, the BDPA found violations related to information, prior to processing DPIA and record of processing activities duties (articles 13, 30, 35 GDPR). Consequently, the Authority imposed a fine of 100,000 euros to defendant.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 48/2022 of 4 April 2022

Another BDPA ruling on the compliance with GDPR of passenger's temperature checks in a Belgian airport during COVID-19 epidemic crisis.

Authority started a second investigation due to use of thermal cameras for temperature check in Brussels Airport (i.e. the first defendant). In this case, passengers were first going through a first-line control implying use of thermal cameras. If passengers' temperature exceeded two times above 38°C they were redirected to a second-line control carried out by a different undertaking active in the medical field (i.e. the second defendant). This temperature survey is manual and passengers were asked to fill a questionnaire. Answers to questionnaires were stored for five years and some personal data were transferred to flight operators (e.g. name and flight number). Before the BDPA, defendants disagreed on their qualification under GDPR for processing related to second-line control. Litigation chamber concluded that both defendants were joint controllers for these processing operations due to converging decisions of the defendants regarding purposes and means of the processing. In particular, the second defendant determined essential means of the processing such as storage duration and recipients of the data. Regarding lawfulness of processing operations, the BDPA found it unlawful for same reasons as in decision 47/2022. Thus, defendants infringed articles 5, 6 and 9 GDPR. In this regard, authority noticed that absence of legal framework was mentioned in the DPIA of first defendant. This conclusion should have led the defendants to the conclusion that processing cannot take place. According to litigation chamber, second-line control constituted a large-scale processing of sensitive data on which decisions are taken. However, defendants decided not to carry out a DPIA for this processing (infringement of Article 35 GDPR). The first defendant also infringed article 13 GDPR. Consequently, the BDPA imposed a fine of 200,000 euros to the first defendant and of fine of 20,000 euros to the second defendant.

DATA PROCESSING AND PRIVACY IN ADMINISTRATIVE PROCEEDINGS

State Council, judgment 253.589 of 27 April 2022

Council State rejected a demand to suspend and annul a decision to impose a sanction against an agent of the Justice administration (SPF Justice).

The claimant is an agent of the defendant (i.e. a prison warden). She filed a claim in order

to obtain suspension and annulation of a sanction decision pronounced by the defendant's executive committee due to the claimant's multiple failures to inform in due delay of absences for medical reasons (i.e. *ex officio* resignation). First, she argued that the decision was, among others, taken in violation of good administration principles and duty of meticulousness. She pointed out that her medical treatment implied use of antidepressant causing distraction and drowsiness which increased the difficulty to fulfill her administrative obligations. According to her, on pain of committing a manifest error of assessment, duty of meticulousness imposed to defendant to investigate reasons of her failures to notify medical absences in due delay. State Council nevertheless considered that duty of meticulousness does not imply that an administrative authority can investigate, in defiance of privacy and medical confidentiality, in order to find if the health status of the agent prevents her to comply with administrative duties. Second, she argued that the defendant committed indirect discrimination because the disciplinary rules are the same for agents failing to comply with their administrative duties for medical reasons or negligence. According to her, the defendant could request information on agents' health status to the administration of medical expertise. Court however highlighted that defendant cannot investigate on medical reasons of an agent's absences. Furthermore, the administration of medical expertise cannot communicate this information to the defendant. Under article 9 GDPR such data can only be processed by health professionals. Finally, as agents are allowed to demonstrate during disciplinary process that health related circumstances exonerate them for their liability, no discrimination can be established.

Council of State, judgment 253.677 of 6 May 2022

State Council decided to suspend the execution of a decision to grant a public procurement for reasons related to compliance with data protection rules.

This case concerns the decision of a public undertaking entrusted with public services missions within health care (i.e. the defendant) to grant a public procurement for subscription to a digital tool for analysis and feedbacks of hospital activities. Claimant is an unsuccessful tenderer which requested the suspension of this decision. In essence, the claimant considered, *inter alia*, that defendant has failed to prove in court that it had verified compliance of tender for successful tenderer with minimum requirements of a public procurement for the designation of a data processor. State Council first recalled that as a controller of sensitive data, defendant must verify that, in accordance with article 28 GDPR it only designates processors providing, *prima facie*, sufficient guaranties to comply with the GDPR. Secondly, the Council of State noted that, in this particular case, compliance with GDPR constitutes a minimum requirement of the public procurement since it was mentioned in the technical specifications of the procurement. Hence, the defendant had to control this tender regularity requirement before granting the procurement. In practice the defendant only mentioned "regularity: yes" in its tender analysis report. State Cuncil highlighted that, as pointed-out by the claimant, the press relayed information about a smart analytics sub-processor of the successful tenderer based in Russia. However, tender did not explicitly mention existence of this sub-processor or the difficulties arising from this situation with regard to the case law of the EU Court of Justice. In light of such known elements, the defendant's reasoning about the regularity of the tender was insufficient. The defendant therefore failed in its duties to verify tender regularity and to give reasons for its decision. Consequently, the State Council suspended the defendant's decision.

RIGHT TO ERASURE – RIGHT TO BE FORGOTTEN

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 38/2022 of 17 March 2022

The BDPA examined a complaint from a former lawyer who had been disbarred following criminal convictions, who criticised Google for refusing his request to dereference various press articles relating to the convictions.

Claimant filed a complaint against various Google entities for refusing to dereference a series of URLs visible on the Google search engine. These URLs were links to press articles with references to offences committed by the appellant as a lawyer and for which he was subsequently disbarred. Google refused to dereference the links because information published was relevant to the claimant's professional activity (he had been employed as a lawyer by a consultancy firm after his disbarment). DPA first considered its jurisdiction over various Google entities involved (§35-84). It then assessed whether Google had violated Article 17 of the GDPR. On the basis of various criteria, such as

(i) the fact that the press articles came from recognised publishers, (ii) the claimant did not deny the truthfulnessof the facts, (iii) the claimant was a lawyer before (iv) he was about to be rehabilitated from his convictions and (v) he played a key role in local public life at the time of the facts in view of his capacity as a lawyer, Chamber decided to close the case without further action. Seriousness, their recent nature and their relevance to the claimant's activity and status were decisive in the DPA's assessment.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 84/2022 of 24 May 2022

OBFG (i.e. a Belgian Bar Association in Belgium which represents lawyers registered in some regions of the country) filed a complaint against two lawyer referral websites.

OBFG considers that its members (lawyers) are listed on these sites without any legal basis for processing, without their knowledge and that informations contained therein is often erroneous. Association also points out that these websites include false comments directed to registered attorneys. The BDPA first confirmed that the OBFG, as representative association of lawyers, had right to file a complaint under Belgian data protection law (i.e. the Belgian Act of 30 July 2018). Chamber then found that defendant, which operates two disputed sites, had no basis for lawful processing of listed lawyers data. According to the BDPA, the processing cannot be based on a contract, nor on the lawyers' consent, nor on the controller's legitimate interest. Chamber then found that the defendant did not comply with Articles 13 and 14 of the GDPR (obligation to provide information). Additionally, its privacy policy and its cookies charter were incomplete and unclear (failure to clearly state the parent company, incomplete list of processing purposes, unclear and questionable data retention period, no mention of the recipients of the processed data). Chamber also considered that Articles 5.1. a) (fairness of the processing), 5.1.b) (purpose limitation) and 5.1.d) (data accuracy requirement) of GDPR are not respected. Consequently, BDPA obliged defendant to suspend all data processing, to review its privacy policy, to destroy the illegally processed data. An administrative fine of 5,000 euros is also imposed.

Constitutional Court, judgment 52/2022 of 31 March 2022

Court is invited to compare, with regard to the possibility of applying for rehabilitation - which entails the deletion of certain data from the criminal record - persons who have been convicted of a criminal offence and persons who have been interned for their offences.

Under Belgian law, rehabilitation allows effects of a criminal conviction to be removed provided that 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 prohibits the rehabilitation of a person who has been interned. Constitutional Court was asked to answer the question of whether this legal provision violates the principles of equality and non-discrimination, in particular because continued registration of the internment decision in criminal records reveals the person's past and mental state (i.e. an element of his or her private life). On the one hand, Court considers that insofar interned persons are not convicted and do not suffer the consequences of such a conviction, it is justified that interned persons cannot benefit a rehabilitation measure. The legal provision is therefore valid. On the other hand, the Court considers it disproportionate that there is no possibility for internees to have the internment decision removed from the criminal record, even though this decision also pursues the objective of social rehabilitation. According to this ruling, absence of a legal regime can allow to request that internment decisions no longer appear in criminal records and are no longer accessible to the administrative authorities is discriminatory and contrary to right to privacy.

PUBLIC DATABASES

Brussels Court of Appeal, Brussels Markets Court, 19th Chamber A, judgment of 23 February 2022

Court of Appeal considers that the protection of individuals with regard of processing of personal data implies a clear division of responsibilities. Hence, the Court decides to ask the EU Court of Justice about the interpretation to be given to the term "controller" enshrined in Articles 4.7 and 5.2 GDPR.

Ruling concerns an appeal by Belgian State against the decision of the BDPA's litigation chamber (decision 38/2021 of 23 March 2021), which issued a reprimand to the Belgian State (in particular Ministry of Justice). The Ministry of Justice had refused to grant the request for eras-

ure made by a citizen who had seen some of his personal data published in the Belgian Official State Gazette, following an error made by his Notary. Markets Court raised questions about the notion of data controller insofar the case involved several potential controllers: the notary, who filed deed to State Gazette, registry of the court which received the deed, and the State Gazette which published the data without any power of control. The Court therefore wonders whether the notion of "subsequent" or "successive" controller is enshrined in GDPR. With this judgment, the Court asks the EU Court of Justice for a preliminary ruling on whether an official journal of a Member State which is responsible for publishing, without exercising any discretion, official acts and documents communicated by third party public bodies (which have themselves processed the personal data contained in these acts/documents) should be considered as a data controller within the meaning of GDPR. Court also asks, in case of a positive answer, whether only Official Sate Gazette is obliged to comply with the principle of accountability (Article 5.2. of the GDPR) or whether all successive controllers are obliged to do so.

Belgian Constitutional Court, arrest No. 33/2022 of 10 March 2022

This action for annulment brought before the Belgian Constitutional Court is directed against a law of 22 May 2019 which amends some legal provisions relating to the management of police data.

The applicant (i.e. the *"Ligue des Droits Humains*" ("Human Rights League"), raised a single *plea*, divided into seven branches, relating to violation of the 'police' directive and other Belgian and European instruments enshrining the rights to privacy and data protection. Applicant considered that the contested law infringed those various instruments as regards (1) the special categories of personal data, (2) the interconnection of police databases, (3) the processing of data subjects' data who are the subject of an administrative police measure, (4) the storage of personal data and (5) the direct access to intelligence and security services to general national database. In substance, the applicant considered that were involving a violation of legality to extent that it is not sufficiently clear, precise and foreseeable, which are necessary conditions for an interference with right to privacy and to data protection. In view of the length of this arrest, we limited our assessment to some points of the reasoning of Constitutional Court. With regard to the special categories of data, the Court found that the contested provisions were sufficiently precise to the extent that the purposes of their processing and their storage duration were determined. Moreover, safeguards were put in place to ensure that the data were adequate. The law entails adequate protection in this regard. With regard to rules applicable to interconnection of police databases, the Court considered that law contained essential elements of the processing and that – given the relatively technical nature of this interconnection – it was not meaningless that implementing measures could be taken by the Ministers of Interior and of Justice. Furthermore, specific guarantees governed this interconnection. In particular, the Court noted that these implementing measures had to be published in the Belgian Official Gazette which constitutes an additional transparency measure. Finally, as regards consultation of general national database, the Court considered that the system implemented by the law ensured (see B.56 et seq.) a fair balance between the protection of privacy and the defence of national security. The court thus decided to dismiss judicial action.

DATA PROCESSING BY PUBLIC AUTHORITIES

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 80/2022 of 13 May 2022

The BDPA ruled on distribution of an e-mail address to third parties in the context of sending a bulk e-mail.

In this case, defendant had sent three e-mails to a mailing list for an urban development project, using the "carbon copy" ("cc") function and not the "blind carbon copy" ("cci") function. Data Protection Authority's inspection service initially found several breaches of GDPR, including breaches of the principles of lawfulness and purpose limitation to the extent that the data processing was further incompatible with the original purposes. Two findings of BDPA's decision can be highlighted. First, the BDPA considers that the sending of an e-mail address to a mailing list is not *per* se a further processing of data for a purpose incompatible with the original purpose. On the contrary, BDPA ruled that this should be interpreted as a separate processing of data requiring a separate lawfulness basis. In this case, the defendant could not rely on any basis of lawfulness present in the GDPR. Second, Litigation chamber recalled that publication by claimant of her e-mail address on the internet had no effect on the personal data qualification of such infor-

mation. Thus, it did not prevent the application of principles of GDPR to defendant. Accordingly, Contentious Chamber issued a reprimand to defendant.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 105/2022 of 17 June 2022

The BDPA ruled on a complaint for processing by tax administration of client's data of a person exercising a profession subject to professional secrecy.

In this case, the Belgian tax administration had carried out an investigation at the complainant's premises and used the accounting data collected in the course of this investigation to initiate two proceedings against the complainant's clients. The administration later accused them of fraud. In this case, the claimant directed its action towards the tax administration because he considered that it had no interest in collecting and processing the personal data of his clients. The BDPA's findings in this case relate more to the admissibility of the action than to the substance of the dispute. Litigation chamber noted that the complainant had a commercial interest in the action, since it concerned his clients' data, but did not have a specific interest in the protection of his clients' personal data. The BDPA noted that the fact that the data concerned were those of the plaintiff's clients did not automatically mean that the plaintiff had a specific interest in the data processing carried out by the tax authorities. The BPDA considered that the clients' data did not become the plaintiff's data merely because they were processed in the context of his self-employed activity. The BDPA therefore decided to reject the complaint.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 31/2022 of 4 March 2022

A person filed a complaint for the identification of the number plate of a car following a parking ticket, followed by a parking tax notice.

The BDPA was asked to rule, among other things, on the question of legal succession between various public authorities. In this case, the plaintiff received a municipal tax after having received a parking ticket. Until 1 January 2020, an autonomous entity of the city of Kortrijk (the "régie communale autonome" "Parko", hereafter referred to as the 'RCA') was authorised to process the number plate 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 city of Kortrijk was in breach of GDPR when it relied on "Deliberation 02/2016" to process its number plate, as it was not the recipient of this normative text, unlike the RCA. Kortrijk city argued, in the judgment, that it was the legal successor of the RCA and was therefore entitled to process the plaintiff's personal data. In this case, BDPA considered that a legal succession could take place as long as purpose for which personal data were processed remained unchanged. Furthermore, it recalled that in Belgium, such a succession could only take place if a specialized committee had a chance in order to assess succession and to determine whether the new controller presented sufficient guarantees with regard to the processing of data of the data subjects. After having examined the facts, the BDPA considered that these conditions had not been met by the city of Kortrijk. Therefore, it had failed to inform complainant about the succession with the RCA. Since the legal basis for the data processing carried out by the city of Kortrijk was lacking, BDPA decided to impose the defendant to bring the processing into compliance.

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

PROTECTION OF PERSONAL DATA BY LOCAL AUTHORITIES

CNIL, Deliberation MEDP-2022, 5 May 2022, deciding to make public 22 formal notices issued against municipalities

With this deliberation, the CNIL makes public 22 formal notices issued against French municipalities, and reminds all public actors, and specifically local authorities, of the importance of appointing a personal data protection officer (DPO). The appointment of a DPO remains an obligation for all public actors operating perso-

nal data processing in accordance with Articles 37 et seq. of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR).

The news regularly reports on issues to protect personal data within large private digital companies. However, public actors and local authorities also collect and use innumerable personal data as part of their public service missions (civil *status*, census, housing, assistance to individuals, video protection, etc.). In addition, the use of data tends to increase in the context of "smart cities" projects that are developing increasingly throughout the country and demonstrates the importance of ensuring effective protection of citizens personal data. However, it appears that many municipalities do not comply with their obligations in this area, particularly with regard to the appointment of a DPO. It is in this context that the President of the CNIL sent, on 2 June 2021, a letter to 22 municipalities that had not yet appointed a DPO. Faced with the lack of response from these municipalities, the CNIL decided on 25 April 2022, to give these municipalities formal notice to appoint a DPO within four months. This appointment is a legal obligation to which any public actor carrying out personal data processing is subject in accordance with articles 37 and following of the RGPD.

With regard to the elements indicated in the deliberation, the publicity of these formal notices is justified in several respects. First, because of the "central role" that DPO can play for governance of personal data within local authorities, and sensitivity of the data processed by them. The importance of the DPO's role is expressed, as the CNIL reminds us, through his or her various missions, ranging from information and advice to cooperation with the CNIL's departments. Secondly, it appears that the failure of the municipalities concerned to appoint a DPO is implicitly affected by an aggravating circumstance, insofar as they have had four years, from the entry into force of Law No. 2018-493 of June 20, 2018 on personal data protection and transposing the RGPD into domestic law, to appoint one. At last, CNIL considers this situation serious enough, to inform the users of these municipalities and remind all public actors of the importance of designating a DPO within their organization.

Finally, this decision is above all a reminder to all public actors who have not yet appointed a DPO. The CNIL, aware of the difficulties that smaller municipalities have in financing their RGPD compliance, reminds us that it is still possible for several public authorities to pool their efforts (for example, various initiatives to centralize data protection activities at the intermunicipal and metropolitan level), as well as to outsource to specialized actors (lawyers, consulting firms, specialized companies). Moreover, this deliberation echoes a recent study by the Data Publica observatory, which revealed that only 47% of French municipalities had appointed a DPO by 1 January 2022 (The Data Protection Officers. Study of appointments in French municipalities: *https://www.lagazettedescommunes.com/telechargements/2022/06/etude-rgpd-dpo-observatoire-data-publica-juin-2022.pdf*). The reflection to be made is that small municipalities, with a population of less than 3,500 inhabitants, have the most difficulty in appointing their own DPO.

DATA PROCESSING BY NATIONAL EMPLOYMENT AGENCY

Decree No. 2022-955, 29 June 2022

This decree is issued in application of the provisions of article L.5312-13-2 of the Labor Code, created by article 268 of the Law No. 2020-1721 of 29 December 2020 of finance for 2021. The purpose of this decree is to strengthen the prerogatives of the agents in charge of fraud prevention at Pôle emploi in the context of their missions to control the declarations of job seekers. The decree broadens the spectrum of data accessible to Pôle emploi agents, allowing them to exercise their right of communication to information held by "certain organizations and companies, in particular banking institutions, energy suppliers and telephone operators [...]".

Monitoring unemployed persons was instituted by law No. 2008-758 of 1 August 2008 on the rights and duties of job seekers, and has been continuously reinforced since then. The decree of 29 June 2022 allows *Pôle emploi's* authorized and sworn agents to collect new information on the beneficiaries of social benefits paid by *Pôle emploi* from new organizations such as banking institutions, telephone operators, and gas and electricity suppliers. The collection of these data falls within the scope of the "right of communication" provided for in paragraph 2 of Article L.5312-13-2 of the French Labor Code. This right of communication allows certain agents of *Pôle emploi* "to obtain, without being opposed to professional secrecy, the documents and information necessary for the control of the sincerity

and accuracy of declarations made as well about documents authenticity produced with a view to the allocation and payment of allowances, aid and all other benefits provided by Pôle employ".

The decree under review specifies the terms and conditions for exercising this right of communication. Firstly, given the sensitivity of the data processed in the context of the fight against social benefit fraud, the right of communication is only available to Pôle emploi agents who are approved and sworn in accordance with the provisions of article L.5312-13-1 of the French Labor Code. Secondly, concerning the content of the request. It must specify on the one hand, "the nature of the legal or economic relationship existing between the person to whom the request is addressed and the persons who are the subject of the request". In other words, the agents in charge of fraud prevention must be able to prove that the person being audited has a link with the organization to which the request is addressed (holding a bank account, subscription, etc.). In addition, the request must specify "at least one of following criteria: geographical location, level of activity or level of resources received, which may be expressed in terms of financial amount or the number or frequency of transactions carried out or payments received; [or] method of payment or remuneration". Finally, it must be specified "the period, which may be divided up, but may not exceed eighteen months, to which the request relates". Lastly, with respect to mode of transmitting and conserving data, it is stated that informations must be communicated on a digital medium, in a secure manner, and "kept for a period of three years from the date of receipt and until the exhaustion of the channels and time limits for appeal against the recovery of undue payments, administrative sanctions or criminal convictions resulting from controls carried out on the basis of this information.

However, the decree does not specify whether algorithmic devices can be used to provide decision support in order to fraud prevention officers. From a prospective point of view, and in view of the extension of tools for monitoring the unemployed, it is legitimate to think that the use of algorithms in service of social fraud will develop for years to come. For example, within tax fraud framework, data mining has been the subject of major developments and some elected officials are considering extending these processes to the fight against social fraud (Law proposal, adopted by the Senate, implementing various urgent measures to fight against social fraud, No. 122: *https://www.assemblee-nationale.fr/dyn/16/textes/l16b0122_proposition-loi*).

DEVELOPMENT OF DIGITAL IDENTITY

Decree No. 2022-676, 26 April 2022

The purpose of Decree No. 2022-676 is to allow French Government to estabilish a new personal data processing system intended to simplify the identification or authentication of holders of a national identity card (CNI) with an electronic component, with public institutions and private organizations. In addition, it repeals previous decree No. 2019-452 of 13 May 2019 authorizing the creation of an electronic means of identification called "Authentication en ligne certifiée sur mobile" (ALICEM).

Decree 26 April 2022 marks a new step in the process of creating a national digital identity in France. The previous initiative, which aimed to set up the ALICEM system, was not completed due to, among other things, too many user concerns about privacy. Digital identity system included the use of artificial intelligence and more specifically facial recognition. The new system authorized by the decree and called "Service de garantie de l'identité numérique" (SGIN) does not include any facial recognition system and was validated by the Commission National Informatique & Liberté, in a deliberation No. 2022-011 of 10 February 2022 (*https://france-identite.gouv.fr/assets/files/CNIL-D%C3%A9lib%C3%A9ration-2022-011_SGIN-France-Identit%C3%A9-2.pdf*).

The SGIN system referred to in the decree allows users with a smartphone that has "a contactless reading device", i.e. an NFC chip, to download a mobile application that allows them to identify themselves or authenticate themselves electronically "with online services offered by providers linked by agreement to FranceConnect, providers linked by agreement to the data controllers". Thanks to the application, the user can generate "electronic certificates containing only the identity attributes that he or she deems necessary to transmit to the third parties of his or her choice". In accordance with Article 1 of the decree, the Minister of the Interior and the National Agency for Secure Titles jointly implement the processing and are jointly responsible within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (RGPD).

Secondly, the decree, in Article 2, sets out

the spectrum of data processed by the SGIN system. Not surprisingly, it is possible to find all of the data present in the electronic component of the CNI, with the exception of digitized images of fingerprints, allowing the identification of the user himself (surname, first name(s), date of birth, postal address, etc.), but also data allowing "the identification of the document held by the user"; data "relating to the history of transactions carried out by the user, within the limit of a maximum number of transactions determined by the data controllers"; and finally the identifier of the smartphone used. Access to this data is restrictive and only concerns "the agents of the General Secretariat of the Ministry of the Interior and the National Agency for Secure Documents". Moreover, these agents are "individually designated and specially authorized by their director". In addition to the agents belonging to the organizations responsible for data processing, the decree provides (Article 3) for the possibility of accessing certain data, which are listed exhaustively, for "the France Connect teleservice" as well as the teleservice providers linked to it, or to the Ministry of the Interior or the ANTS. Moreover, regardless of who receives the data, access is "limited to the need to know" and any operation of "creation, consultation, use, revocation and deletion of the electronic means of identification" remains recorded for a period of three years on the servers of the data processors. The data can be used as evidence in the event of a dispute.

Thirdly, the decree sets out the methods of storing the data. The above-mentioned data are stored in two ways. First, the data are stored on the server of the Ministry of the Interior and the ANTS. These are kept for a period of 5 years from the last use of the service by users, or immediately deleted in case of uninstallation of the application. In addition, the data are automatically deleted after two years of inactivity. Secondly, the data are stored and encrypted locally on the user's mobile device. As with server storage, the data are kept on the terminal for five years from the last time the user uses the service.

Finally, in accordance with the provisions of the RGPD, users have a right to information, access, rectification of data, as well as the right to limit the processing.

SCOPE OF THE RIGHT OF ACCESS TO ADMINISTRATIVE DOCUMENTS

Council of State, 10th – 9th chambers, 3 June 2022, No. 452218

In this case, State Council rules on the scope of users' right of access to correspondences of a mayor and local elected officials. While certain categories of correspondence sent or received by a local elected official may be qualified as administrative documents and subject to Article L.300-2 of the Code of relations between the public and the administration (CRPA), others are not, notably "correspondence from local elected officials which cannot be considered as emanating from the municipality since they express, in particular, personal positions or positions taken within the framework of the free exercise of their elective mandate".

The case concerned a dispute between several citizens and the commune of Arvillard. The citizens requested that the mayor provide them with "all the emails exchanged with the local elected officials concerning the deliberations of October and November 2016" relating to a micro-power plant project, on the basis of Articles L.300-2 et seq. of the CRPA, which set out the regime for the right to access and communicate administrative documents. Following the Mayor's refusal to communicate these documents, the citizens appealed to the Grenoble Administrative Court for the annulment of the Mayor's decision to refuse. By judgment No. 1804016 of 5 March 2021, the Grenoble Administrative Court granted the citizens' request and ordered the Mayor to communicate the requested documents. By a summary appeal and a supplementary memorandum, registered on 4 May and 28 June 2021, the municipality of Arvillard applied to the Conseil d'Etat for the annulment of the Grenoble Administrative Court's judgment.

The question put to the judges of the Council of State was to determine whether the communications of the local elected representatives had the character of administrative documents (and were therefore communicable on the basis of Article L.300-2 of the CRPA).

In this case, State Council made a distinction between two categories of communications. According to judges, it is according to correspondence content that it will be possible to qualify them as administrative documents. Thus, Court specifies in its third recital that "only correspondence sent or received, in context of functions exercised on behalf of the municipality, by the mayor, his deputies or the members of the municipal council to whom the mayor has delegated part of his functions, have the character of administrative documents". Conversely, "correspondence from local elected officials which cannot be considered as emanating from the mu-

nicipality since they express, in particular, personal positions or positions taken in the context of the free exercise of their elective mandate" do not have the character of administrative documents.

Finally, State Council considered that administrative court of Grenoble had erred in law by qualifying the mayor's correspondence as administrative documents "without investigating whether they had been issued or received on behalf of the municipality and were not intended to express the personal or political positions of elected officials in exercise of their elective mandate".

DATA PROCESSING BY POLICE AUTHORITIES

Constitutional Council, No. 2022-993 QPC, 20 May 2022

On 20 May 2022, the Constitutional Council ruled on the constitutionality of Articles 60-1 and 60-2 of the Code of Criminal Procedure, resulting from Law No. 2019-222 of 23 March 2019 on programming 2018-2022 and reform for justice, which allow the public prosecutor and judicial police officers to obtain communication of or the access to connection data.

The priority question of constitutionality (QPC) concerned contents of Articles 60-1 and 60-2 of Code of Criminal Procedure, which allow access to and communication of connection data to the public prosecutor and judicial police officers in the context of flagrance investigations. The main complaint against above provisions was that the processing of connection data, which "includes in particular data relating to the identification of persons, their location and their telephone and digital contacts, as well as online public communication services they consult", could infringe on people privacy concerned, and should therefore be subject to prior review by an independent jurisdiction.

Constitutional Council, while recognising existence of a risk to privacy individuals, relied on several elements to reject complaint. Indeed, it states that the disputed provisions of the Code of Criminal Procedure "strike a fair balance between the constitutional objective of tracking down the perpetrators of offences and the right to privacy". For the Constitutional Council, this conciliation is rightful for various reasons.

Firstly, these provisions were adopted by legislator in the context of an objective of constitutional value: that of "finding the authors of offences". Secondly, methods of requisitioning connection data provided for in Articles 60-1 and 60-2 are accompanied by adequate guarantees. Indeed, "these provisions only allow data requisitions in context of a police investigation into a flagrant crime or a flagrant offence punishable by a prison sentence". Furthermore, the flagrance investigation remains limited to eight days, and can only be extended for a further eight days if it "concerns a crime or an offence punishable by a prison sentence of five years or more and if the investigations cannot be deferred" and with the prior authorisation of the public prosecutor. Finally, these requisitions are only possible "on the initiative of public prosecutor, a judicial police officer or, under latter's supervision, a judicial police agent", and are carried out under the supervision of a judicial magistrate who ensures 'the proportionality of the investigative acts with regard to the nature and seriousness of the facts' in accordance with Article 39-3 of the code of criminal procedure.

Constitutional Council, No. 2022-1000, DC, 13 August 2022.

Following a referral from the deputies of the National Assembly, the Constitutional Council ruled on the constitutionality of several provisions of Law No. 2022-1159 of 16 August 2022 adapting French domestic law to European Union law with regard to the prevention of the dissemination of content of a terrorist nature. This law modifies the Law No. 2004-775 of 21 January 2004 for confidence in the digital economy by adapting it to the Regulation (EU) 2021/784 of 29 April 2021 on the fight against the dissemination of terrorist content online (TCO Regulation). It includes a new mechanism to combat the dissemination of terrorist content on the Internet. The new Articles 6-1-1, 6-1-2, 6-1-3, 6-1-4 and 6-1-5 of the amended Law No. 2004-775 are concerned by the referral. They provide for the possibility for the Central Office for Combating Information and Communication Technology Crime (OCLCTIC) to issue injunctions to host service providers to block or remove terrorist content. Recipients then have one hour from receipt of the injunction to block or remove the targeted content. If the injunction is not complied with, the providers are liable to a criminal sanction of one year's imprisonment and a fine of 250,000 euros.

The plaintiffs argued that the device instituted by Law No. 2022-1159 would be contrary to the Constitution by disproportionately infringing on the freedom of expression and communication enshrined in Article 11 of the Declaration of the Rights of Man and the Citizen of 1789. This

freedom of expression and communication is a principle inherent to constitutional identity of France. Its respect should thus be controlled by Constitutional Council in the event of adaptation of French domestic law to European law. Disproportionality existing between the infringement of freedom of expression and communication results because provisions in question provide for a non-suspensive recourse for supplier against the injunction intended for him. According to the petitioning deputies, the injunction formulated by OCLCTIC, an administrative authority attached to Central Directorate of Judicial Police, would reduce the freedom of its addressee without any prior judicial review or effective remedy being available to the recipient.

In its decision, the Constitutional Council declares the articles of Law No. 2022-1159 referred to in the referral to be in conformity with the Constitution. The Council declares that the contested provisions do not infringe the principle of freedom of expression and communication, but rather aim to limit the abuses of which terrorist content is a part. It dismisses the complaint of lack of judicial review by reiterating that the determination of the terrorist nature of the content targeted by an injunction is not left to the sole discretion of the administrative authority. The latter must indicate precisely the terrorist content and give detailed reasons for its characterization as such in the injunction it issues. Indeed, a qualified person within the Regulatory authority for audiovisual and digital communication (Arcom) must systematically be informed of injunctions addressed to providers, whose regularity it controls as a member of an independent administrative authority (AAI). The qualified person within Arcom has the power to make recommendations to the administrative authority issuing the injunction. In the event that the latter does not follow them, the qualified person within Arcom has a summary appeal to the administrative judge or a request to be judged within 72 hours. Thus, an administrative blocking or removal order is subject to review by an independent authority and is subject to rapid cancellation by the administrative judge.

In addition, the judicial review of the legality of the injunction can also be carried out at the initiative of the recipient. The addressee of an injunction has the right to appeal to the administrative judge, specially provided for by the Law No. 2004-775, in addition to the classic appeal in summary proceedings before the administrative court. This specific recourse requires the administrative judge to rule again within 72 hours from the date of referral. According to the Council, this short time limit helps to guarantee the effectiveness of the recourse available to the recipient. The complaint of lack of effective recourse for the host service provider is thus rejected by the Constitutional Council.

Constitutional Council, No. 2022-1000, QPC, 17 June 2022.

Based on a previous application of a priority question of constitutionality, the 20 June 2022, the Constitutional Council ruled on the constitutionality of Article 99-3 of the Code of Criminal Procedure, as resulting from Law No. 2016-731 of 3 June 2016 (also known as Law Urvoas), strengthening fight against organized crime, terrorism and their financing, and improving the efficiency and guarantees of criminal proceedings. It also ruled on Article 99-4 as issued by Law No. 2004-204 of March 9th, 2004 (also known as Law Perben II) adapting justice system to changes in crime. These two articles provide a framework access power of the examining magistrate and judicial police officer executing a letter rogatory, to all kind of documents and data in the context of a judicial investigation. Access could not be denied on the basis of professional secrecy.

More specifically, priority question of constitutionality targeted access power to "computer system or processing of personal data" where "connection data issued by a lawyer and related to the use of an electronic communications network or service" are concerned. The applicant criticized these provisions framing this special case of requisition, for they grant the power to order the communication of connection data when an investigation could concern any type of offence. According to the applicant, the fact that such power is neither justified by urgency nor limited in time, would result in a disregard for the right to privacy provided for in article 2 of Declaration of Rights of Man and of the Citizen from 1789. An additional critic is directed against the alleged lack of legitimacy of the examining magistrate and the judiciary police officer acting by letter rogatory, as an investigating judge would not constitute an independent jurisdiction.

Nevertheless, Constitutional Council confirmed constitutionality of this provision. Unsurprisingly it starts reiterating that the examining magistrate itself is a jurisdiction whose independence is guaranteed by the Constitution. Therefore, his requests, as well as the requests issued by a judiciary police officer acting by let-

ter rogatory, do not suffer the alleged lack of independency. As such, a judicial police officer is only entitled to requisition connection data within the limits of the letter rogatory, as set by the independent examining magistrate.

More importantly, Constitutional Council demonstrates that Articles 99-3 and 99-4 of Code of Criminal Procedure reconcile, in a balanced manner, rights, both of constitutional status, of privacy and of finding the perpetrators of crimes pursued by legislator. This balance is rooted in the system's respect for criminal procedure. Exercise of access power granted to the examining magistrate or to judicial police officer authorized by a letter rogatory is in keeping with separation of prosecution and investigation functions. The latter is the responsibility of the examining magistrate, while the former is not. Except in the case of a suspected crime or certain misdemeanors in which a judicial inquiry must be opened, it is up to the public prosecutor to proceed with this opening by means of an indictment addressed to the examining magistrate. The public prosecutor controls the offence orientation of the investigation. Also, Where public prosecutor does not request a judicial investigation, only constitution of a civil party in the criminal trial allows for its opening in accordance with Articles 85 and following of the Code of Criminal Procedure. Thus, any data examined during the investigation phase cannot be used to monitor the commission of an offence outside the scope of the investigation established at the opening of the judicial inquiry. In addition, the opening of a judicial investigation is mandatory only for offences specified by law. Thus, neither judicial information systematization, nor the concentration of the functions of prosecution and investigation will lead to a disproportionate infringement of right to privacy of the accused.

Finally, requirement that the judicial investigation be carried out within a reasonable period of time in view of the seriousness of the acts with which the accused is charged, as provided for in Articles 175-2 and 221-1 of the Code of Criminal Procedure, justifies the dismissal of the applicant's complaint according to which there is no time limit.

Court of Cassation, Criminal Division, No. 21-83.710, 12 July 2022.

The Criminal Division of the Court of Cassation has ruled on the compatibility of Articles 60-1, 60-2, 77-1-1 and 77-1-2 of the Code of Criminal Procedure with European Union law. These articles establish the regime under French domestic law for the rapid retention and access to traffic and location data by the police in the context of a flagrante delicto investigation.

The author of the appeal maintains that the use by the examining chamber of evidence obtained through the preventive, generalized and undifferentiated collection and storage of traffic data and location data of the accused is not compatible with European Union law. Furthermore, the collection of personal data and their retention in the context of a flagrante delicto investigation would be neither targeted nor subject to the authorization and control of an independent authority. This would result in a violation of EU law.

The Court of Cassation partially upheld the arguments put forward in the appeal. Notably, it notes that Articles 60-1, 60-2, 77-1-1 and 77-1-2 of the Code of Criminal Procedure do not provide for prior review by an independent administrative authority, or by an independent court, of the data requisition. It concludes that French procedural law is incompatible with European Union law, insofar as the Court of Justice of the European Union has made such prior control a condition for authorizing data requisition (CJEU, 2 March 2021, aff. C-746/18, H.K./Prokuratuur).

On the other hand, Court of Cassation reiterates that it is up to the examining chamber to control the regularity of the means of obtaining evidence when it is seized in this sense by the applicant subject to criminal proceedings. The investigating chamber must therefore check that the requisition of data has been carried out in compliance with the purpose of combating serious crime and relates to targeted and regularly stored data. In this respect, the Court of Cassation specifies that "*the interpretation that would exclude from the scope of rapid retention data retained for the purpose of safeguarding national security would deprive its purpose, which is to allow national authorities, in the fight against serious crime, to access data that have not been retained for this purpose*". In addition, the control of regularity implies verifying that the requisition respects limits of what is strictly necessary for investigation. In other words, the requisitioned data must be necessary to establish the truth and proportionate to seriousness of suspected crimes. Above all, Court of Cassation indicates that the irregularity of a data requisition only leads to a regime of relative nullity of the act concerning the accused. This finding of nullity on the basis of Article 802 of Criminal Code is itself conditional on the applicant having suffered harm as a result of the irregularity. When the irregularity has not irrevocably affected the

rights of the accused, the Court of Cassation specifies that such prejudice is established under two conditions. On the one hand, the applicant must demonstrate an unjustified interference with his privacy and the protection of his personal data. On the other hand, the applicant must show that the categories of data concerned and duration of access to them were not in this case limited to what was strictly justified by the needs of the investigation. In short, irregularity of a data requisition is not an absolute cause of nullity.

LEGAL STATUS OF A SOCIAL NETWORK PAGE IN THE CONTEXT OF A SERVICE CONCESSION

Council of State, 2nd and 7th, 16 May 2022, Commune de Nîmes, No. 459904

The Council of State has clarified the legal regime applicable to a social network page whose management was entrusted to a concessionaire whose contract has not been renewed.

When it entrusts a service provider with management of a public service or a public works operation, administrations may be led to assign administration rights of pages dedicated to these activities on social networks. The municipality of Nîmes had concluded such an agreement with the company Culturespaces for the management of the city's Roman monuments. As the concession has come to an end, it has not been renewed. However, despite the administration's requests, the company didn't return all the tools it was responsible for, namely a promotional film, decorations and, therefore, the pages dedicated to these monuments on social networks. The municipality of Nîmes applied to the administrative judge for an interim injunction, which allows any useful and urgent measure to be taken in order to ensure the continuity and proper functioning of the public service, which does not hinder the execution of an administrative decision. As this request was rejected, it was up to the Council of State to rule on the inclusion of the social network pages among the assets that were to revert to the public entity at the end of the contract and on the regime for this transfer.

The assets built or acquired within the framework of a concession are, when they are necessary for the public service mission, the property of the public entity. At the end of the agreement, these assets, qualified as return assets, must in principle be returned free of charge to the latter. One of the main contributions of the decision is to qualify a page on a social network as a return asset. Intangible property has already been qualified as such, such as computer software, but the uncertainty lay precisely on the point of knowing whether the access rights to a page on a social network constitute property. State Council accepted this qualification because, this is essential point, concession left it up to company to promote monuments, notably "via social networks". In fact, the age of pages had enabled creation of a relatively large network of subscribers that it would have been very difficult for the new concessionaire to reconstitute in the short term. It was therefore understood that the disputed pages constituted an element of the concession necessary for the proper functioning of the public service and should revert to the public entity at the end of the contract.

Without directly pronouncing on legal nature of rights of administration of a page on a social network, administrative judge thus remits a pragmatic approach to this question, centred on public services needs, which constitutes after all the cardinal point of the regime of return assets and, more broadly, of the law of public property.

CONTENTIOUS STATUS OF A LINK TO AN INTERNET PAGE

Council *of State, 9th and 10th chambers, 3 June 2022, Association* Pornostop, *No. 453794*

The Council of State recently clarified the way in which information published online by the administration could be seized by the judge. At issue was the refusal to remove a link to a website. The decision of the Council of State is interesting in several respects. On the one hand, it settles the question of the nature - regulatory or not - of a decision relating to Internet links. Secondly, and more importantly, it implicitly recognises that such a decision can be appealed, which was not at all obvious.

As they are interconnected, government departments are logically bound to interact, which is reflected on the Internet by links to the websites of the various administrations. It was in relation to such a link that the Pornostop association filed a petition with the Council of State. It challenged the Prime Minister's refusal not to remove a link from the website www.jeprotegemonenfant.gouv.fr to the onsexprime.fr platform, which is managed by Santé publique France, govermental public institution. It considered that this platform conveyed an approach to sexuality, and in particular pornography, that was contrary to principle of neutrality of the public service.

As the State Council does not have jurisdiction in principle, it had to ensure that the application fell within one of the cases covered by article R. 311-1 of the Code of Administrative Justice (CJA), in particular that concerning appeals "against regulatory acts of ministers and other authorities with national jurisdiction". The issue was therefore to determine whether the refusal to remove an Internet link constituted a regulatory decision or not. The public rapporteur considered, and the Council of State agreed, that such a decision was devoid of any regulatory nature and constituted rather a decision of the case, i.e. neither an individual nor a regulatory decision. Indeed, if the existence of an Internet link is on a site open to the public has, by definition, a general and impersonal scope, the administrative judge considers that it is not strictly speaking a regulation, nor even a measure of organisation of the public service - of which it is nevertheless a tool. The application should therefore have been sent to Paris Administrative Court.

By forwarding application to competent administrative court, Court implicitly but necessarily accepts that the refusal to remove an Internet link is a decision that can be appealed. Indeed, article R. 351-4 of the CJA stipulates that, even if it is not competent to hear the case, an administrative court must reject "conclusions that are clearly inadmissible and cannot be covered in the course of the proceedings". Now, it was not absolutely certain - without being surprising - that the refusal to remove an Internet link constitutes an act likely to be referred to the administrative judge, especially when it refers, as in this case, to the site of another administration. This decision is not uncontroversial, since it amounts to placing the burden on the administration to check the updating of the sites of other services to which it refers, which may seem excessive. It is likely that the State Council did not want to prohibit users from challenging links placed online as a matter of principle, while leaving it up to the judge in charge of merits of this case to construct a balanced system. It will be interesting to follow the development of this case before the administrative Court of Paris in order to measure exact weight of requirements burdening the administration.

CENSURE OF THE OBLIGATION TO BRING A CASE TO COURT BY ELECTRONIC MEANS

ECHR, 5th section, 9 June 2022, *Xavier Lucas vs France*, No. 15567/20

Justice has not escaped the digitalization of public action. Different levels of jurisdiction have thus designed their own referral platforms - Télérecours for administrative justice, e-barreau for the judicial authority - which have gradually become more or less compulsory. It is this last feature that Mr Xavier Lucas challenged before the European Court of Human Rights. Court of Cassation had in fact quashed and annulled a decision of the Court of Appeal which had ruled on his application even though it had not been transmitted by the appropriate digital means.

The law of the European Convention on Human Rights does not prohibit in principle use of dematerialization of judicial proceedings. On the contrary, the Court is "convinced that digital technologies can contribute to a better administration of justice". However, it ensures that a certain balance is maintained, because "in applying the rules of procedure, the courts must avoid both excessive formalism, which would undermine the fairness of the proceedings, and excessive flexibility, which would result in the removal of the procedural requirements laid down by law". It is precisely this balance that it has struggled to find in the position of the French courts.

Admittedly, rule was predictable. It results from a combination of Article 1495 of the Code of Civil Procedure (CPC) - relating to appeals against an arbitral award, as in this case - with Article 930-1 of the same Code, to which it refers. Article 930 requires the court to be seised electronically.

On the other hand, it seemed difficult to place the burden of the system's malfunctions on the applicant. While the Court admits that "it is neither unrealistic nor unreasonable to require the use of such a service by legal professionals, who have long made extensive use of computers", it requires the public justice service to provide sufficient information and functional tools. In this case, the e-barreau platform did not really allow the registration of Mr Luca's request, whose lawyer would have had to provide inaccurate information in order to fill in a form that was not adapted to his case. The judgment adds that the Court of Cassation should have shown flexibility in the face of the significant difficulties encountered by the applicant by not imposing conditions for referral that he was unable to meet. By failing to take account of the specific nature of applicant's situation in order to attenuate the rigour of the procedure, the French court imposed on him "a disproportionate burden which breaks the fair balance between, on the one hand, the legitimate concern to ensure compliance with the formal conditions for bringing a

case before the courts and, on the other hand, the right of access to the courts".

Court's judgment is to be welcomed. By censuring the excessive formalism of the Court of Cassation, the European judge guarantees that the digitisation of judicial procedures remains a vector of progress without constituting a new obstacle for the litigant.

PROVISION OF PUBLIC DATA, ALGORITHMS, AND SOURCE CODES BY THE ADMINISTRATION

Prime Minister circular, No. 6264/S, 27 April 2021

This circular from Prime Minister, define the politic of data, algorithms, and source codes in the state's administration.

In continuity of French public action transformation, services of Prime Minister elaborated this circular, in order to rule the way that state's administration should treat their numeric data. Indeed, as the use of numeric data increase in the decision-making processes of administration, new standards of transparency should be respected, if we still want to call our states democracies.

In this matter, the French law only impose to the administration, when she use algorithms to take an individual decision, to indicate that this decision has been taken on the base of an algorithm. In this case, public decision also indicates the means by which, his recipient could be aware of the way that the algorithm has been applied to treat his situation (See the articles L.311-3-1 and R.311-3-1-1 to R.311-3-2 of the Code of relations between the public and the administration). In other terms, the administration keeps a passive posture, in which she has to wait for the demand of the citizen, before provide him the numeric data used in the decision-making processes. Moreover, these rules only apply for individual decisions from administration (like advantages, or sanctions), and not for general settlements, whereas these ones are also elaborated with the use of numeric data.

In this context, Prime Minister circular considers that state's administrations have to adopt a pro-active posture in the provision of their numeric data used in decision-making process. This mean for these administrations to provide to citizens, on a website, the data, algorithms, and source codes, which contribute to the process of public decision, even before the decision has been taken. This provision of numeric data will be established gradually in each minister of the french government, and will be coordinated by the general administrator of data, algorithms and source codes.

The interventions registered on this differ among each other in manifold respects this circular. First, by her nature, the circular doesn't create a right that can be invocated by citizens in front of a court. She only provides guidelines for the state's administration, and not for the decentralize administration (like cities, departments, and regions). That mean if a state administration fails to provide the numeric data which serve to elaborate public decision, citizens can't use the circular to suit this administration before public court, to force her to disclose her numeric data. Then, according to this circular, the provision of the data, algorithms, and source codes is more motivated by objectives of administration's efficacity and economic growth, rather than imperatives of transparency. Indeed, the principles goals of this provision, are to share the practices that simplify the decision-making process, and to enable private actors to reuse strategic public data. Finally, even if circular promotes a pro-active posture of State administrations, in the provision of their numeric data, we see that citizens are still far to be in capacity to ask administration for account, for using numeric data for decision-making process.

Opinion from Commission for Access to Administrative Documents (CADA), 23 June 2022, No. 1454

The French CADA consider that the source code of a public service's website is not communicable to citizens, if it has been created by a private provider, without being fully yield to the administration.

In this case, a citizen asked the national center for university and school works (CNOUS), a public establishment attached to the ministry of higher education, the communication of the eVote website's source code. This platform has been created by a third party, for the account of the CNOUS, to collect the french student's vote for the election of their representants in the regional delegations of the CNOUS.

Despite the progress in terms of transparency in the use of numeric tools for public decision-making process, the french law admit some exceptions for the communication of source codes and algorithms to citizens. These exceptions are listed by the articles L.311-4 to L.311-6 of the Code of relations between the public and the administration. They notably concern, the national defence secrecy, the business secrecy, and the respect of the intellectual propriety rights.

Moreover, when the administration doesn't own the source code elaborated by a third person, citizens can't impose to the administration the communication of this source code. Indeed, if the administration does communicate it, this would be a violation of the propriety right of the source code's owner. In this situation, administration can only ask the communication of this source code to its owner. But if this one refuse to communicate it, the administration can't see her responsibility engaged.

After having recalled this legal context, the CADA doesn't precise if her opinion is favorable or unfavorable for the communication of the source code owned by a third party. She only advises the administration to characterize whether trade secrets or intellectual property rights hinder the communication of the source code in its entirety. Indeed, as this situation is not strictly ruled by the law, CADA wants to let flexibility for the administration, to deal with these requests on a case-by-case basis. However, CADA consider that if the source code is related to a voting operation, his communication is very important for the confidence of citizens in the results of the vote. In such circumstances, CADA asks government to rule in order to strike a fairer balance between administrative transparency guaranteeing the trust of citizens, and the business secrecy and intellectual property.

GERMANY

edited by

Felix SCHUBERT, Ph.D. candidate in comparative public law, in cotutelle at the University Panthéon-Assas (Paris 2) and at Saarland University in Germany; research assistant at the Chair of French Public Law at Saarland University; "Volljurist"; "Diplomjurist"

USE OF THIRD-PARTY DATA BY THE STATE

Higher Regional Court of Frankfurt, court order 1 HEs 427/21 of 22 November 2021

The Higher Regional Court of Frankfurt had to decide whether information gathered by the FBI through controlling the supposedly secure crypto-messenger "Anom" was appropriable in German criminal procedures.

In this case, the Higher Regional Court of Frankfurt ordered the continued validity of the claimant's detention on remand, considering that he was strongly suspicious of illegal drug trafficking and of forming a criminal organisation. The strong suspicion was mainly based on chat protocols of conversations that the claimant had with another suspect, using the crypto-software "Anom". The findings were completed by surveillance and raids, leading to illegal drug labs, drug storage locations, the seizure of illegal drugs and vehicles with built-in secret storage facilities for drugs. The Court motivated its decision by the very high probability with which these findings would be admissible as evidence. After having teared down the service provider "Phantom Secure" offering encrypted communication technology used by criminal organisations to coordinate their activities, the FBI wanted to gain again access to the communication of criminal organisations. Therefore, the FBI had developed its own app (Anom App), with the help of an informant and the Australian Federal Police. After an installation of the Anom App, devices were end-to-end encrypted and the device could only be used for communication with other Anom users. A master-key allowed the FBI to then decrypt and download sent messages. The FBI made the gathered information available for law enforcement agencies of different countries, among them the German Federal Police (*Bundeskriminalamt*). The suspect argued that this evidence was inadmissible for several reasons. Among others, because the FBI had, according to the claimant, actively taken part in the criminal activities, under violation of Article 6 paragraph 1 of the European Convention on Human Rights (ECHR). The claimant also argued that not individualised users, but all users of the app were under surveillance, without any concrete suspicion. The Court underlined that the standard for the admissibility of evidence collected abroad differed from evidence collected in Germany. The legal basis for the use of evidence gathered by the FBI would be Section 479, paragraph 2 of the German Criminal Procedure Code. A procedure that is different from those in Germany would not affect *per se* the admissibility. An inadmissibility could only result from certain exceptions, for example in case of violation of binding guarantees of public international law in favour of individuals like Article 3 or 6 ECHR or of general principles of the rule of law in the meaning of the public policy. Or when the purpose of the investigation was to bypass German law. According to the Court, the FBI did not actively take part in criminal activities by making available a supposedly secure crypto-messenger, because the decision to use such a technology for criminal activities was the sole responsibility of the users. According to the

Court, the app did not either serve the purpose of penetrating the users' privacy. Since the app made a normal use of the device on which it was installed impossible, and since its acquisition was available only to a restricted circle of users, it could be expected that the app would be used in the field of organised crime. The error about the supposedly secured communication was not sufficient to constitute a violation of the human dignity or the public policy. Also, German authorities did not on purpose take part in the Anom schedule to bypass German law otherwise applicable.

Federal Supreme Court, court order 5 StR 457/21 of 2 March 2022

The Federal Supreme Court had to decide on the appropriability of information obtained by French authorities through surveillance of the crypto-messenger-service EncroChat.

The claimant in this case was sentenced to 5 years' imprisonment for drug trafficking. His conviction was based amongst others on information that the German state attorney had obtained from French authorities. This information had been discovered during a surveillance operation of the crypto-messenger-service EncroChat. French law enforcement agencies came across EncroChat during several investigations in 2017 and 2018 where suspects used mobile phones encrypted with EncroChat. Due to the encryption, an assessment of these devices by law enforcement agencies was not possible. The district attorney of Lille therefore requested the French Counter-Cyber-Crime-Centre in 2018 to infiltrate the EncroChat network. The investigators learned that these mobile phones were advertised with a guarantee of anonymity, and a double operating system (OS) permitting to switch between the Android OS and the EncroChat OS. No legally existing manufacturer could be identified. Distributers and buyers of theses phones were selectively chosen. French investigators managed to obtain a copy of a server linked to EncroChat domains. They found more than 66,000 SIM-cards of which more than 10,000 had been used in France. They were also used in the Netherlands, Spain, the UK, Germany and Italy. Because of the alleged anonymity, users communicated openly about organised drug trafficking, for example about transporting 60kg of cocaine. In 2020, French authorities managed to insert spyware into the EncroChat network, using a technology that was kept confidential for reasons of national security. Europol transferred data obtained by these means to German law enforcement agencies. Some of this data incriminated the claimant and an investigation led to his conviction. The claimant challenged his conviction before the Federal Supreme Court for several reasons. First, he argued that provisions of the German Criminal Procedure Code were not respected by French authorities. Second, he argued that the core of his privacy was violated by the surveillance. Third, heo invoked that he was the subject of illegal mass-surveillance. The Court replied that the appropriability in German criminal proceedings of evidence obtained by foreign law enforcement agencies did not require a respect of the German Criminal Procedure Code. The legality of investigative measures had to be analysed according to the law of the foreign (French) State. The secrecy of parts of the French investigation for national security reasons did not render them illegal. Also, a violation of the national or European public policy could not be found. The Court did not follow the claimant's argument of an illegal unfounded mass-surveillance of all EncroChat users. Because these specified mobile phones, that were not available on the normal market and that generated considerable costs for acquisition and maintenance, gave sufficient grounds to suspect their users to be involved in organised crime. Also, by monitoring the claimant's communication on the planning and execution of criminal activities, the French authorities did not violate the core of his privacy. The secret surveillance was proportionate, because the offence in question weighed particularly heavily and because the clarification of the facts would have been particularly difficult or impossible. The Court therefore admitted the appropriability of the evidence and rejected the claimant's challenge.

Higher Regional Court of Frankfurt, court order 3 Ws 369/21 of 20 July 2021

The Higher Regional Court of Frankfurt had to decide whether a German car producer had to disclose to law enforcement agencies GPS-data sent from a car used by a fugitive.

The claimant in this case, a German car producer, was ordered by a German state attorney to disclose GPS-data of a car produced by the claimant and suspected to be used by a fugitive. The car was indeed equipped with a multimedia-system permitting among others its user to locate the car, or to automatically share its position with rescue services in case of an accident. This system transmitted via a pre-installed SIM-card, a part from the location, also the current mileage status, tire pressure and the fuel level to

the claimant's server, as well as to the user's mobile phone. The claimant challenged the state attorney's order before the Regional Court of Gießen, but lost at first instance and challenged this decision before the Higher Regional Court of Frankfurt, which also found the challenge unfounded. The state attorney's order was based on Section 100k (entered into force in April 2021) of the German Criminal Procedure Code which permits to collect usage data from those who make tele-media available as a business. The Court reminded that usage data are, pursuant to Section 15 of the German Tele-media Act (*Telemediengesetz, TMG*), personal data that are generated by using a tele-media-service and which are necessary to make the usage possible or to invoice this service. The Court drew a parallel of the car's multi-media-service with mobile phones. It found that the multi-media-service was a "tele-media-service", because it was a service automatically transmitting data from the car to the server. Data which then served as basis for information that would subsequently be transmitted to the user. The Court did not follow the claimant's argument of an exclusive machine-to-machine communication, because data was made perceptible for the user, like the location of the user's car. Also, GPS-data could be requested by the state attorney, because the wording of Section 100k comprises expressly "location data" and because a location could also be determined by GPS-data and not only by cell-ID tracking (as argued by the claimant). The Court therefore upheld the state attorney's order.

Administrative Court of Cologne, court order 6 L 1277/21 of 1 March 2022

The Administrative Court of Cologne had to decide whether the new provisions of the Act to Improve Enforcement of the Law in Social Networks (Netzwerkdurchsetzungsgesetz, NetzDG) violated EU-law.

The new Section 3a of the NetzDG obliged providers of social networks to verify if certain contents, that have been the object of complaints, and that have been deleted or to which the access has been restricted, might indicate a criminal offence. In case of such indications, the contents have to be transferred, together with certain information pertaining to the user, to the Federal Police (Bundeskriminalamt). The new Section 4a of the NetzDG makes the Federal authority for Justice (Bundesamt für Justiz) the competent authority for supervising the respect of the provisions of the NetzDG. Google Ireland, as operator of the social network Youtube, requested (amongst others) the Administrative Court of Cologne in a summary procedure to declare these new provisions inapplicable to Google. The Court found indeed that Section 3a of the NetzDG was inapplicable to Google because it violated EU-law, namely the country-of-origin-principle of the Directive on electronic commerce, according to which the legal requirements for providers of electronic services established in a member State of the EU are to be determined by the law of State of origin. The German State could not invoke exceptions to this principle, because it had not proceeded to the consultation and information procedure, nor were the conditions of an emergency procedure fulfilled. The Court further found that Section 4a of the NetzDG was inapplicable to Google, because it violated the Directive on audiovisual media services, pursuant to which the competent media-authority for the control of service providers needs to be legally and functionally independent. The Bundesamt für Justiz though is subordinated to the Federal Ministry of Justice and Consumer Protection, and bound by its instructions. It therefore is not independent at all.

APPS USED BY THE ADMINISTRATION FOR TRACKING OF SOCIAL INTERACTIONS

Higher Regional Court of Rostock, court order 17 Verg 6/21 of 11 November 2021

The Higher Regional Court of Rostock had to decide on the legality of a direct award to the manufacturer of a tracking app of social-interactions despite the offer of another manufacturer of a product that did not fulfil all requirements of the performance specification.

The defendant in this case, the State of Mecklenburg-Vorpommern, intended in February 2021 to decrease the Covid-19 lock-down. After experiences with tracking of social interactions on the basis of attendance lists in paper form, the easing of the lock down should be accompanied by a more efficient form of tracking. The defendant did online researches on apps that would fit such a purpose. The defendant found several products during his online research, but did not esteem them eligible for an award, except for the so-called "Luca"-App of a third party (culture4life GmbH). Without public tendering and without requesting other offers, the defendant therefore acquired the "Luca"-App. The claimant then initiated review proceedings against this decision. He lost though, because his app in its initial form did not allow any efficient

tracking of social interactions. The claimant challenged the rejection of his review proceedings before the Higher Regional Court of Rostock. The Court confirmed however the previous decision and underlined that the claimant's app did not allow to fulfil the requirements of Section 28a, paragraph 1, No. 17 and paragraph 4 of the Act on the Prevention and Control of Infectious Diseases (Infektionsschutzgesetz, ISFG) that had become part of the performance specification for the award. According to Section 28a, paragraph 1, No. 17 and paragraph 4 of the ISFG, the administration can order the processing of personal data of clients, guests or participants of events so as to track their social interactions. This data has to be transferred by the organisers of events to the competent health authority. The claimant's app worked as follows. During the installation, no personal data needed to be entered. The QR-Code of an event could be scanned to "check-in" to the event. Warnings of occurred infections in the context of a certain event were indicated by the health authority on the claimant's server. The app regularly updated these warnings and notified its users about potential contacts with infected people. The notified user could subsequently voluntarily enter his or her personal data and grant to the health authority access to this data. Only then, the personal data would have been available to the health authority. The event organiser had no access to the data, nor could he transfer them to the health authority. According to the Court, the defendant could legitimately require the software to work immediately and did not need to offer to the manufacturers the possibility to adjust their products.

Higher Regional Court of Rostock, court order 17 Verg 4/21 of 11 November 2021

In another decision from the same day, the Higher Regional Court of Rostock had to decide on the legality of the direct award despite the offer of another manufacturer whose product fulfilled the requirements of the performance specification.

The claimant in this case was another software manufacturer challenging the direct award of the tracking app contract by the State Mecklenburg-Vorpommern to the manufacturer of the Luca-App (culture4life GmbH), although the claimant had manifested its interest beforehand by email. The claimant lost its review proceedings against the direct award, but then challenged this decision before the Higher Regional Court of Rostock. According to Section 97, paragraph 1 of the Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen, GWB), public tendering is necessary before the award of a contract, except if provided for otherwise by statutes according to Section 119, paragraph 2 of the GWB in conjunction with Section 14, paragraph 2, sentence 2 of the Regulation on the Award of Public Contracts (Verordnung über die Vergabe öffentlicher Aufträge, VGV). Such a legal exception, exempting even from negotiation procedures, exists with Section 14, paragraph 4, No. 3 of the VGV if extremely urgent circumstances in the context of unpredictable events do not permit to respect deadlines provided for other procedures. The defendant argued in favour of this exception. The Court found however, although not provided for by statutes, that even in case of an extreme emergency, a "light competition" procedure could be due, including at least the obligation to verify the offers already made to the awarding authority. Since the defendant had not respected such a "light competition" procedure, the Court found that the contract was awarded illegally and therefore null and void.

Administrative Court of Osnabrück, court order 1 B 24/21 of 15 June 2021

The Administrative Court of Osnabrück had to decide whether a public authority could legally advertise exclusively the tracking app of a private manufacturer without suggesting alternatives.

The health authority of the city of Osnabrück chose in March 2021 to use the Luca-App (see above) in order to track social interactions, to the disadvantage of different manufacturers of similar apps, like the claimant in this case. The city of Osnabrück, the defendant in this case, then published on its website dedicated to the Covid-19 pandemic (www.corona-os.de) amongst others also information on the Luca-App. It was expressly written: "This is why the city and the municipality support the use of luca: the luca App is a digital alternative to common data processing, that can deliver us relevant data". It was made clear that an exclusive and extensive use of this specific app should be made by citizens. The claimant requested the defendant in a summary procedure to stop partisanship and one-sided advertisement for the Luca-App. The Court reminded that this would require a violation of the claimant's fundamental rights by the defendant, as well as a concrete risk of repetition of such a violation. The Court then found that the freedom to choose an occupation pursu-

ant to Article 12 of the Federal Constitution was interfered with by the defendant's statements, because they influenced voluntarily the market's condition to the claimant's economic disadvantage. In a next step, the Court verified whether this interference was justified or not (only the unjustified interference would constitute a violation of the claimant's fundamental right). In order to be justified, this interference would require a statutory basis and the absence of errors of assessment. The Court found that section 28, paragraph 1 in conjunction with Section 28a, paragraph 1, No. 17 of the Act on the Prevention and Control of Infectious Diseases (*Infektionsschutzgesetz, ISFG*) could serve as statutory basis, pursuant to which the competent authority can take the necessary measures when it can identify (amongst others) a person who has fallen ill, or a person suspected to fall ill or a person suspected be contagious. Under necessary measures also fall the order to process contact details of clients, guests or participants of events so as to track possible infection chains. The absence of errors of assessments requires that the measure is proportionate. In order to be proportionate, the measure needs first to be suitable to serve a legitimate goal (suitability). Second, it must be necessary to achieve that goal, which means that no other measure would have been equally effective and less disruptive (necessity). Third, the disadvantages must not be disproportionate to the targeted goal (appropriateness). In this case, the Court considered that the measure taken by the defendant was not necessary. Because less disruptive and equally effective measures would have been at hand: namely informing citizens about alternatives to the Luca-App and explaining why exactly the defendant had chosen this specific app. The Court therefore found that the measure was not proportionate, hence that an error of assessment was given. In consequence, the interference with the claimant's fundamental right could not be justified and constituted a violation. The defendant's statements were therefore illegal and the Court ordered the defendant preliminarily to stop partisanship and one-sided advertisement in favour of the Luca-App.

WARNING BY THE ADMINISTRATION OF A FOREIGN SOFTWARE-MANUFACTURER'S ANTI-MALWARE SOFTWARE

Administrative Court of Cologne, court order 1 L 466/22 of 1 April 2022

The Administrative Court of Cologne had to analyse the legality of a public warning issued by a federal authority against Russian anti-malware software Kaspersky.

The claimant in this case was the manufacturer of Russian anti-malware software Kaspersky, requesting in summary proceedings the Federal authority for Security in Information-Technology (*Bundesamt für Sicherheit in der Informationstechnik, BSI*) to refrain from publicly warning against its anti-malware software. The BSI had indeed warned the public against dangers arising from the Kaspersky software and recommended to replace its products by software from other manufacturers. The Court reminded that market players had no right to permanent, unchanged market conditions; that therefore not every information published by the administration would automatically constitute an interference with fundamental rights. The Court also reminded that such an information could constitute such an interference where the State action aimed at individualised companies, where it influenced voluntarily the decisions of market participants, and where it downgraded the market position of the concerned companies. The warning published by the *BSI* fulfilled these conditions pursuant to the Court. The judges found however that the interference was justified and did therefore not violate the claimant's fundamental rights: The BSI had acted on basis of Section 7, paragraph 1, sentence 1 of the Act on the Federal authority for Security in Information-Technology (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*). According to this statute, the *BSI* can address warnings against security gaps in IT-products and services to the public or parties concerned and can recommend security measures or the use of certain security products. Pursuant to Section 7, paragraph 2, sentence 1 of the same Act, the *BSI* can also warn publicly against security gaps in IT-products and services and against malware, as well as mention the concerned product and the manufacturer, when the *BSI* has sufficient indications that the products present a threat to IT-security. Considering the extensive rights granted to anti-malware software, it presents a threat when the necessary high level of trust in its manufacturers is not given anymore. The Court esteemed that the possibility of influence of Russian players, especially the Russian State, on the manufacturer could not be excluded. The Court made reference to the current geopolitical situation and Russia's attack on the Ukraine, which is led also as cyberwar, to conclude that Russian coders could abuse technical possibilities, out of

their own accord, or under external pressure, to corrupt computer-systems in other States. In consequence, the manufacturer could not be trusted anymore according to the Court. In absence of a violation of fundamental rights, the Court rejected the claimant's request.

ACCESS TO SOURCE-CODE USED BY THE ADMINISTRATION

Administrative Court of Wiesbaden, judgement 6 K 784/21.WI of 17 January 2022

The Administrative Court of Wiesbaden had to decide whether a teacher could validly request under the Hessian Data Protection and Information Freedom Act the source code of software used by the administration.

The claimant in this case, a teacher at a Hessian school, requested access to the source code of software used by the Hessian Ministry of Education for a platform providing different services, among others the digital administration of classes and courses or self-learning materials for students. The claimant invoked Section 80, paragraph 1, sentence 1 of the Hessian Data Protection and Information Freedom Act granting a right to access official information (amtliche Informationen). Official information is defined in Section 80, paragraph 1, sentence 3 as records serving official purposes. While the Court admitted that a source code could constitute a record, it denied that it served official purposes and justified this reasoning with several arguments. First, the possession of source code was not necessary for the performance of public tasks. The Court illustrated this argument by underlining that the State of Hesse did not possess the Windows source code, although its IT was mainly based on that operating system. The information of the source code was as little necessary to the fulfilment of public missions as details about pens or doors used by the administration. Second, the rationale of Section 80, paragraph 1, sentence 1 was to control State action. And the quality of the administration's equipment was in principle irrelevant to exercising this control (a part from a justified public interest in case of deficient equipment). What mattered to determine the legality of State action was its content, not its physical basis. Third, the exception of Section 82 No. 2, b of the Hessian Data Protection and Information Freedom Act would apply in any case. According to this Section, access to official information must not be granted if it jeopardizes public security. Since the Court considered that the publication of a source code of software used by the administration would grant individuals with malicious intent access to weaknesses of the software, this publication would endanger the software's IT-security. The Court also considered that the administration's own IT-staff was not sufficiently qualified (due to unattractive working conditions and salaries) to distinguish between security-sensitive and non-sensitive elements of the source code, which would require to hire expensive experts, which could not be refinanced. The Court therefore rejected the claim. An appeal was lodged against this judgement.

ITALY

edited by
Alessandro DI MARTINO, Research Fellow in Administrative Law, University of Naples Federico II
Elio GUARNACCIA, Administrative Lawyer
Alessia PALLADINO, Ph.D in Administrative Law, University of Naples Suor Orsola Benincasa
Luigi PREVITI, Assistant Professor in Administrative Law (RTDA) at University of Palermo

IRREGULARITY OF THE ACT OF APPEAL WITHOUT A DIGITAL SIGNATURE

Council of State's, Plenary Session, No. 6 of 21 April 2022

In this ruling the administrative Council of State's Plenary session confirms the previous cases law, whereby a notified act of appeal without a digital signature constitutes a mere remediable irregularity. Thus, it falls under the scope of application of the Code of Administrative Procedure, pursuant to article 44, paragraph 2. Consequently, the appellant shall re-notify the appeal, even before the judge's order.

In its Plenary session, the Council of State has dwelled on the provisions and principles governing the appeals, including the consumption of the power to appeal.

Dispute arose from the action brought before the Regional Administrative Court of Lazio, by a citizen who contested the order of the State Property Agency (*Agenzia del Demanio*) to make him release the property. The appeal was extended to the decree of the Ministry of Economy and Finance of 29 July 2005, by which the property was assigned to the State Property Agency.

In its judgment of 24 July 2020, No. 8693, the Regional Administrative Court of Lazio seised upheld the appeal, considering the issue as

a question of private law. Therefore, the Ministry of Economy and Finance and the State Property Agency hold an appeal against the decision, by inferring the violation and / or false application of article 2, contained in the Decree of the Ministry of Economy and Finance, enacted on 29 July 2005.

A cross – appeal was held by appellant at first instance. Besides all, he argued that the appeal was filed at Secretariat of State Council only on 29 January 2021, thus beyond thirty-day deadline established for the filing of appeals pursuant to article 94 of the Code of Administrative Procedure. In details, he underlined that the appeal was initially notified without the affixing of the digital signature, but it was subsequently regularized by appellant through a ritual signature and therefore re-notified to the appellant before the expiry of the deadline for proposing an appeal.

This leads up to reflect towards the effective boundaries of the consummation of the power to appeal, which finds a logical prerequisite in the prohibition of splitting appeals.

The State Council Plenary Session rules inapplicability of power consummation to appeal. On the one hand, its filing at the Judge's Secretariat did not follow the first notification. On the other hand, it would be considered just as a repeated notification of the same act, not relevant for the purposes of the ruling.

The Council of State's Plenary session confirms the previous cases law, whereby a notified appeal without a digital signature constitutes a mere remediable irregularity. Thus, it falls under the scope of application of the Code of Administrative Procedure, pursuant to article 44, paragraph 2. Pursuant to article 44 of the Code of Administrative Procedure, the judge should fix a peremptory term for the regularization of the appeal, in accordance with the law.

The autonomous regularization of the appeal by the appellant represents the peaceful application of the principles of fullness and effectiveness of administrative judicial protection (Article 1 of the Code of Administrative Procedure) and of a reasonable duration of the process (Article 2, paragraph 2 of the Code of Administrative Procedure).

Consequently, the appellant shall re-notify the appeal, even before the judge's order.

In conclusion, in response to questions submitted by referring Section, the Courts formulates the following principles of law. Firstly, there is a mere remediable irregularity, with consequent applicability of the regime pursuant to art. 44, paragraph 2, of the Code of Administrative Procedure, in the case of a notified appeal without a digital signature. Secondly, the appellant can directly re-notify it with the digital signature, even before the judge orders the renewal of the notification. Finally, the deadline for filing the appeal, pursuant to the combined provisions of articles 94, paragraph 1, and 45 of the Code of Administrative Procedure, must start from the date of effective notification of concretely deposited appeal.

INADMISSIBILITY OF THE APPEAL SENT TO AN INAPPROPRIATE PEC ADDRESS

Council of Administrative justice for the Sicilian Region, decision No. 707 of 16 June 2022

The Council of Administrative justice for the Sicilian Region rules that the principles expressed by the Plenary Session of the Council of State No. 6/2022 (whereby a notified act of appeal without a digital signature constitutes a mere remediable irregularity) cannot be extended to unfilled appeals. Thus, the Coucil of State stated on the mere remediable irregularity of unsigned digital appeal, but correctly filed online, pursuant to the established rules for the Telematic Administrative Procedure (TAP). As a matter of fact, pursuant to the Digital Administration Code and the Code of Administrative Procedure, all the pleadings must be created in digital format, and lodged in the online information system, except in cases of technical malfunctions.

The Council of Administrative justice for the Sicilian Region essentially confirms the principles expressed by the Plenary Session of the Council of State No. 6/2022, whereby a notified act of appeal without a digital signature constitutes a mere remediable irregularity.

There are cues to rethink the core principles of telematic administrative procedure.

At first glance, it has not been drafted in digital format with digital signature, thus violating Code of Administrative Procedure too.

Pursuant to article 136, paragraph 2-bis, all the acts and measures of the judge, the auxiliaries, staff and parties must be signed with a digital signature. In particular, all the judicial acts must be drawn up in the format of an electronic document signed with a digital signature, in compliance with the requirements established by Article 24 of the Code of Digital Administration.

However, in the light of principles established, an appeal fulfilled in non-digital format isn't affected by nullity (pursuant to art. 1 of the

Code of Civil Procedure), thus the judge can assign to the party a peremptory term for its regularization, pursuant to article 44, paragraph 2, of the Code of Administrative Procedure. Nevertheless, the Court has dismissed the duty of regularization on the grounds of procedural economic, since the inadmissibility of the appeal.

Secondly, the Council of Administrative justice for the Sicilian Region observes that the appeal has not been sent to the appropriate PEC address.

In this regard, the Board does not consider the principles expressed by the aforementioned Plenary: actually, the case law examined by the Council of State is about the appeal without a digital signature, but correctly filed electronically, pursuant to the established rules for the Telematic Administrative Procedure (TAP). Moreover, the Board confirms that the judge, due to specific and motivated technical reasons, may authorize any paper copy.

It follows that since the administrative process is an electronic process, all the documents are not only formed, but also deposited, in an almost "exclusively" digital manner, subject to the precise exceptions referred in article 9, paragraphs 8 and 9, of the Decree of 28 July 2021, on the technical-operational rules of the electronic administrative process.

The digital filing must necessarily be sent at the certified email address specifically authorized to receive appeals. Otherwise, the appeal cannot be considered pending at the judicial office as long as it is not assigned a general register number.

For this reason, the Board dismisses the action as inadmissible.

RESPONSIBILITY OF THE ADMINISTRATION FOR MALFUNCTIONING OF IT PLATFORMS

Council of State, sec. VI, No. 829 of 7 February 2022

The Council of State argues that due to the principle of loyal cooperation between the administration and citizens established by Article 1, para. 2-bis, of Law No. 241/1990, the submission of an application on a telematic platform does not replace one that has already been submitted but assumes a supplementary nature. The ambiguity of the underlying instructions of the computer system platform cannot burden the participant in a selective procedure; therefore, the responsibility for the malfunctioning of the machine belongs to the public administration.

The Council of State annulled the first instance decision of the Basilicata Regional Administrative Court, which ruled that the amendment of the titles for participation in a competition notice implied the invalidation of the previous application and not its mere supplementation. In particular, the first instance court based its decision on the principle of the private individual's self-responsibility; by virtue of the latter, the competitor must bear the consequences of the errors and omissions committed, which in the present case relate to the indication of the qualifications in the application. The Council of State reversed the first instance decision and held that the ambiguity of the instructions for application submission led the candidate into error. In such circumstances, it is the public administration that is responsible for the error, and this by virtue of Article 1(2-bis) of Law No 241 of 1990. The violation of the cited rule implies - in application of the principle of self-responsibility - that the consequences resulting from the presence of ambiguous clauses in the rules governing the selection cannot be attributed to the competitor who, in an unconscionable manner, relied on them.

Garante per la protezione dei dati personali (Italian Data Protection Authority), decision No. 224 of 9 June 2022

The Authority stated, for the first time, that the operator of a website that uses Google Analytics services for statistical purposes, without ensuring compliance with the guarantees of privacy protection of the website visitors, violates the requirements set out in the EU GDPR. Indeed, the decision to use Google Analytics services automatically determines the transfer of the data collected by the operator to the USA, which is a country without adequate levels of data protection.

The case concerned the use of Google Analytics (GA) services by a private company, aimed at obtaining statistical information on the activity of visitors to its website.

In particular, using GA, company collected several significant data, such as those relating to the browser, the operating system and the users' device, their IP address (which have long been considered as a personal data) and the date and time of the visit to the website. Information that can easily be associated with email address, phone number and any personal data inserted in the Google account, if a user access to the website through it.

Following a complex investigation, the Authority stated that the use of GA by the operator

of the website entails the transfer of personal data of visitors to Google LLC, which is based in the United States, a third country that does not guarantee a level of privacy protection adequate to the standards of the GDPR (on this point, see Court of Justice, 16 July 2020, C-311/18, Data Protection Commissioner vs Facebook Ireland Ltd and Schrems).

This conclusion is based on the factual circumstance that, without appropriate measures to transfer personal data, US governmental authorities and intelligence agencies could access and use the European users data for various purposes, thus infringing the guidance provided by the European Data Protection Committee through its Recommendations No. 1/2020 of 18 June 2021.

In the light of the negligence nature of the offence and the actions taken to mitigate the harm suffered by the persons concerned, the Authority warned the company and ordered it to take within 90 days, under penalty of sanctions, the additional safeguards necessary to make the processing of personal data of website visitors compliant with the specific guarantees required by European data protection law.

PORTUGAL

edited by

Luís Manuel PICA, PhD candidate in Public Law at The University of Minho (Portugal); Teaching assistant 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 SIGNATURE OF "STAND-ALONE DOCUMENTS" VS. "CLOSED DOCUMENTS" AND THE THEORY OF THE DEGRADATION OF ESSENTIAL FORMALITIES INTO NON-ESSENTIAL FORMALITIES IN ADMINISTRATIVE PROCEDURE

Judgment of the Administrative Supreme Court of 30 June 2022

Court considered that, even when uploading based on closed files, the submission of bid is only effective with its electronic signature, this being the moment when it is considered complete and submitted to tender, the bidder being finally bound by the commitment made therein. Therefore, it is not because the documents were not signed before they were uploaded to the platform that the Plaintiff ceased to consider itself bound by what was contained therein, which demonstrates the irrelevance of the failure to sign each document separately in relation to the firmness of the commitment it assumed. Post that electronic signature functions, not in question, have been fulfilled (identifying, finalising or confirming and inalterability) the irregularity resulting from the lack of electronic signature of each separate document is considered to have been "absorbed" by the signature of the whole document containing the commitment to participate in the tender procedure.

Therefore, contrary to what was held in judgment under appeal, nothing can be inferred from the grounds used with regard to the non-application of the so-called 'theory of non-essential formalities' to the situation of the absence of a separate signature for each separate document, on the ground that the non-compliance with the formality that is abstractly invalidating - that is, generating the exclusion of the tender - ceases to be invalid if, in the specific case, the interests or values that the omitted formality was intended to protect have been achieved.

In fact, it is clear that the non-fulfilment of the formality provided for in paragraph 4 of Article 68 of Law 96/2015, namely that when the interested party uploads a proposal file onto the electronic platform, the file must be encrypted and signed, using a qualified electronic signature, always results in the exclusion of the proposal. Theory quoted assumes formality that was omitted in this case and the interests that it intends to safeguard and ensure, as well as the circumstances concretely verified.

In this way, it does not appear that irregularity found compromised the procedure or the intended objectives, since the required formality was eventually remedied by affixing the electronic signature to the entire document submitted on the electronic platform, with the addition of the commitment by tenderer to be bound to the public tender, applying "theory of the degradation of essential formalities into non-essential formalities", set out in Article 163(5)(b) of the Code of Administrative Procedure.

JUDICIAL ACCESS TO DOCUMENTS DEPOSITED ON ELECTRONIC PLATFORMS FOR THE EVALUATION OF JUSTICE

Judgment of the Administrative Court of

Appeal (South) of 4 November 2021

The court considered that the judge must perform the measures of proof that he considers necessary to ascertain the truth (Article 90(1) and (3) of the Code of Procedure of the Administrative Courts). However, he should refuse the diligent proceedings that are impertinent or dilatory, as results from his duty of procedural management - Article 90, paragraph 3 of the Code of Procedure of the Administrative Courts and Article 6, paragraph 1 of the Code of Civil Procedure.

The fact is that, given that the documents included in the case-file, which were not contested, provided proof of the essential facts for the decision to be taken on the merits, the Court did not have to proceed to request other documents, to be extracted directly from the electronic platform where the competition procedure took place, in order to prove those facts. As these were not contested and the Court having issued an order in which it decided that the evidence in the case-file was sufficient to consider the merits of the case, and therefore dismissed the production of the other requested means of evidence, namely the request for documents (to be extracted from the electronic platform) containing the Appellant's access records, one cannot conclude that there was an infringement of the principle of inquisitorial proceedings and the provisions of article 90 of the Code of Procedure of Administrative Courts.

Therefore, the judicial order that dispensed with the performance of diligent proceedings requested did not incur in a procedural nullity foreseen in Article 195, No. 1 of the Code of Civil Procedure, since it does not violate the principle of inquisitorial investigation and the provisions of Article 90 of the Code of Procedure of the Administrative Courts. The judge's action is legitimate in the event of refusal of access to documents deposited on electronic platforms, which the judge could access if they were necessary to ascertain the material truth (Article 6(1) of the Code of Civil Procedure).

ACCESS TO COMMUNICATIONS METADATA BY LAW ENFORCEMENT AGENCIES: CHRONICLE OF AN UNCONSTITUTIONALITY FORETOLD

Rulling No. 268/2022 of the Constitutional Court, of 19 April 2022, Case No. 828/2019

The Portuguese Constitutional Court, in a request for an abstract review of constitutionality by the Ombudsman, declared unconstitutional several provisions of Law 32/2008, of 17 July, on the retention and transmission of data to the authorities for the purposes of criminal investigation, detection and repression of serious crimes.

Some of the provisions at issue are articles 4 and 6 of the aforementioned law. These impose on the providers of publicly available electronic communications services or of a public communications network the duty to retain for a period of one year (from the date of conclusion of the communication), in a general and indiscriminate manner (all subjects - including those for whom there is no suspicion of criminal activity – and all equipment is covered, at all times, everywhere), a wide range of data, namely: base data (independently of any communication, allowing the identification of the user of certain equipment - name, address, telephone number) and traffic data (location of the user, location of the recipient, duration of use, date and time, frequency). The Constitutional Court considered that such a rule disproportionately restricts the rights to privacy and informational self-determination, provided for in article 26(1) of the Constitution of the Portuguese Republic.

The article 9 of aforementioned law, on the transmission of such data to police authorities for aforementioned purposes, was also declared unconstitutional: by not providing for a duty of notification which would allow the subjects to know that their data had been transmitted to the public authorities (when it no longer jeopardizes the success of the investigation), made it impossible, in practice, to react and defend themselves judicially against abusive or illicit access to the metadata stored and transmitted. The fact that the law does not provide for the storage of data in Portugal or in another Member State of the European Union also makes such judicial protection difficult. This disproportionately restricts the right to informational self-determination (article 35, nº. 1) and the right to effective judicial protection (article 20, No. 1, both of the Constitution).

The Constitutional Court further considered, in its Ruling 382/2022 (Case Nº. 828/2019), that "the effects of the declaration of unconstitutionality are determined by the Constitution and not by the Constitutional Court and refer to the date on which the unconstitutional rules came into force", a position that that negatively affects the validity of existing evidence in criminal proceedings in which metadata has been used.

THE POWER OF ATTORNEY IN THE PORTUGUESE

PUBLIC CONTRACT LAW

Rulling of the Southern Central Administrative Court of 13 May 2022, Case No. 01637/21.0BEPRT

In this decision, the venerable Judges of the Southern Central Administrative Court - one of the two intermediate courts of administrative and tax jurisdiction in Portugal - ruled, in a judicial review claim, on the themes of the submission of proposals through a proxy in public procurement procedures and the requirements of the power of attorney.

According to articles 56(1), 57(4) and 62(1) of the Public Contracts Code (PCC), the proposal (declaration of willingness to contract under the terms and conditions set out in the tender specifications) and respective documents must be signed by the bidder or by a representative with powers to bind him/her (e.g., a proxy) and submitted directly to an electronic platform used by awarding entity. If the bid is submitted by a proxy, the power of attorney must be offered with the bid and its respective documents, namely to prove that the subscriber has the powers to bind and commit the bidder to it. Such documentation must be signed with the use of a qualified electronic signature (and not through a mere autograph signature - article 54(1), of Law No. 96/2015, of 17 August), and, in case of representation by an attorney-in-fact, the use of a digital certificate belonging to him – to the attorney - is allowed. Any failure in the compliance with the aforementioned rules determines the exclusion of the proposal (articles 146(2)(e) and 148(1) and (4) of the PCC).

Court considered that a proposal submitted by a proxy should be excluded, based on a power of attorney through which the bidder granted him "the necessary powers, individually, in the name and on behalf of the Principal, to sign and submit documents on the Electronic Platforms", upholding that the rules of interpretation (articles 236 and 238 of the Civil Code) do not allow the conclusion that the bidder has granted the attorney-in-fact powers to bind him/her, but only to represent him/her in the signing and submission of documents on electronic platforms (acts referred to in articles 68 to 70 of Law No. 96/2015, of 17 August). Also according to the Court, a power of attorney that only grants powers to sign documents is valid (sufficient) to physical documents, but not to electronic documents (which are signed by the affixation of an "electronic signature", "advanced electronic signature" or, as required by the PCC, a "qualified electronic signature").

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 SIGNATURE

Supreme Court, Third Chamber, Contentious-Administrative. Case 78/2022, 27 January 2022, proc. 1414/2020

The possession of an electronic certificate of a legal person issued by a trusted certification authority, certifies that the natural person in whose favour it is issued holds its representation, without it could being questioned by any Administration.

In the present case, the individual appeals against an administrative act of the Department of Infrastructures and Mobility of the Autonomous Community of Galicia, whereby he is considered to have withdrawn from an administrative appeal procedure relating to the termination of contracts for regular public transport for special use.

The raison d'être of the decision is found in the fact that administration considers that individual had not adequately complied with requirement that had been made.

Specifically, Administration had requested a notarised power of attorney in favour of person acting on behalf of the individual within administrative procedure, which must be provided by means of an electronic office if notary electronically signed it or, in other case, through the paper register.

In response to the request, the individual provided a simple copy of the notary deed relative to a sale of shares and formalisation of corporate agreements. In these actions, contained in notarial deed, person who was acting in the administrative appeal was appointed as Managing Director and Chairman of the Board having "all the functions and powers corresponding to the Board of Directors (…) except those that cannot be delegated by law".

This simple copy would have been submitted electronically despite the lack of notary electronic sign.

In view of this circumstance, the Regional Court, in the previous instance, had considered

that the notary deed provided by the individual would be indicative of the organic representation of the company within the scope of the corporate purpose, but not of the (voluntary) representation in the administrative procedure.

On the other hand, it was concluded that the individual, being a legal person, had not complied correctly with his obligation to interact electronically with the Administration, even though there were provided two systems for submitting the notary deed requested. The first one by the use of electronic office if the deed was electronically signed by notary. And the second, presenting notary deed, not electronically signed by the notary, in a public office in order to be compared and digitalised by public worker for its submission.

The Supreme Court, however, does not accept this point of view, ruling that:

- The representation contained in the notary deed submitted by the person administered is sufficient for the lodging of an administrative appeal in the light of the Capital Companies Act, as there is no standardised list of these means in the Administrative Procedure Act.

- The Administration cannot tax means of rectification, but the person concerned may respond to the requirement by using "any of the legally recognised means that are effective to correct it, whether or not they have been mentioned in the requirement act to him by the Administration".

- The mere availability and use of an electronic certificate, issued by a competent authority, which allows a legal person to act as attorney, means that the documents and documents signed electronically using said certificate will be understood to be submitted by said legal person, in accordance with article 7.4 of Law 59/2003. Not surprisingly, before issuing the certificate, the certifying authority must verify that the applicant reliably accredits that he or she is represented in accordance with the provisions of art. 13.2 of Law 59/2003. Therefore, the Supreme Court concludes that the "natural person who has a digital certificate to electronically sign documents on behalf of a legal person has reliably demonstrated before the corresponding certifying authority that he or she holds such representation and, therefore, cannot be questioned by another Administration or administrative body on occasion of each specific action".

ELECTRONIC OFFICE

Supreme Court. Third Chamber, Contentious-Administrative. Case 638/2022, 30 May 2022, proc.165/2021, Fifth Legal Basis

The determination of the minimum content and services that all Spanish administrations must include in their electronic offices falls within the State's competence for the basic regulation of administrative procedure.

On 2 April 2021, Royal Decree 203/2021, of 30 March, came into force, approving the Regulation of action and operation of the public sector by electronic means. Regulatory development of Acts number 39 and 40/2015.

The Government of Autonomous Community of Catalonia lodged a direct appeal of illegality against several precepts of this regulation. One of them was Article 11, paragraphs 1 and 2, which establishes the minimum content and services that the electronic offices of any Administration must have.

This provision is considered by the appellant to infringe the possibility of self-organisation of the different Administrations by predetermining the content of their electronic offices. At the same time, it would be a regulatory provision without legal backing in view of Article 38.3 of Law 40/2015, which states that each Administration shall determine the conditions and instruments for the creation of electronic offices.

However, the Supreme Court accepts the thesis of the procedural representation of the State, confirming the legality of this article, determining that:

- Sections 2, 4 and 5 of Article 38 of Law 40/2015 establish a series of general principles and requirements for the operation of electronic offices, which institute the basis on which Article 11 of Royal Decree 203/2021 establishes its development.

- These provisions do not carry out an exhaustive regulation, but rather a minimum regulation, allowing the addition of other contents by the rest of the Administrations.

- The minimum content required by the State would fall within the scope of the basic regulation attributed by Constitution to State with respect to administrative procedure in Article 149.1.18 for the purposes of guaranteeing common treatment of citizens by all Administrations.

ADMINISTRATIVE DOCUMENTS MANAGEMENT

Supreme Court. Third Chamber, Contentious-Administrative. Case 638/2022, 30 May 2022, proc.165/2021, Fourteenth and Fifteenth Legal Basis

Illegality of the provision of Royal Decree 203/2021 regulating the conservation of all documents submitted by citizens prior to its approval and legality of its regulation regarding the conservation of documents submitted by citizens in an administrative procedure in process when they cannot be returned to them at the time.

On 2 April 2021, Royal Decree 203/2021, of 30 March, came into force, approving the Regulation of action and operation of the public sector by electronic means. Regulatory development of Acts number 39 and 40/2015.

Government of Autonomous Community of Catalonia lodged a direct appeal of illegality against several precepts of this regulation. One of them was the first transitional provision, which states that two years after entry into force of Royal Decree, documents on a non-electronic medium in the possession of the registry assistance offices of which an authentic electronic copy has been made and incorporated into the corresponding electronic file may be eliminated.

However, in order to do so, the mentioned provision established that it would be necessary for all administrations to notify the corresponding classification authority beforehand, together with a risk analysis, the specification of the guarantees of conservation of the electronic copies and compliance with the conditions required by the National Security Scheme, the transparency regulations and other applicable regulations.

In view of this, State's legal representation determines that the contested provision seeks to guarantee the same treatment for all citizens, while the documents subject to destruction on which the rule is based do not refer to internal organization of Administrations, but to the relations between the latter and the citizens, as they affect their legal sphere.

However, Supreme Court considers that this provision is contrary to the legal system after determining that it refers to all documents that were submitted prior to the entry into force of the Royal Decree, irrespective of the time, the type of procedure in which they are included or their processing status. This approach leads court to conclude that it is not intended to guarantee same treatment for all citizens, but is purely organisational in its approach from the point of view of document management and purging.

Consequently, the first transitional provision would be contrary to Article 150 of the Statute of Autonomy of Catalonia, which guarantees the power of self-organisation of Autonomous Community.

In addition with this first additional provision, there is also an appeal against to Article 53 of Royal Decree 203/2021, which provides that documents submitted by interested individuals on paper or portable electronic document storage devices, when is not possible return them at the time of submission. After being digitized and/or incorporated into the electronic file, must be kept and made available to them for six months or such longer period as may be established by each Administration regulation.

Once this period of time has elapsed, they may be eliminated, unless otherwise stipulated by sectorial regulations.

However, in this case, in contrast to the first additional provision, the greater specificity of the eventuality referred to in Article 53 leads the Supreme Court to consider that, now, it is the regulation of a facet of citizens' relations with the Administration that seeks to safeguard common treatment for all citizens in accordance with Article 149.1.18 of the Constitution. In this case, the possibility for citizens to retrieve, for a certain period, documents that they have had to leave in the possession of an administration.

ACCESS TO SOURCE CODE

Juzgado Central de lo Contencioso-administrativo No. 8 (Central Administrartive Court number 8), case 143/2021, 30 December 2021, appeal number 18/2019

Denial of access the BOSCO's Source Code.

In the case of the BOSCO system, in Spain, it is a system that was implemented by the Spanish public administration to increase efficiency in identifying citizens eligible to receive state aid on electricity bills payment. The Civio Foundation (NGO), for its part, developed an alternative application to help citizens identify whether or not they were eligible for the aid, and during its use, it identified potential errors within the BOSCO application. After a first administrative appeal before the Council of Transparency and Good Governance, Civio appealed to the Central Administrative Court to get access algorithm source code and to determine if there was indeed an error or not. According to Civio, the impossibility of accessing the source code of algorithmic decision-making affects the ability to check whether a given final result has been obtained through biased reasoning that does not comply with the law, and therefore its knowledge is essential. Source code opacity, Civio helds, affects not only the rights of parties involved in an administrative or judicial procedure, but also con-

stitutional counterweights that serve as reciprocal controls between the powers of the State.

In its judgment 143/2021 of 30 December 2021, the Central Administrative Court refused access to the source code. The court understands, in the first place, that the actions of the BOSCO system are inserted in an investigation phase of the administrative procedure –a phase previous to the proper decision–, whose purpose is to verify compliance with requirements previously established by the aforementioned regulations. The court makes a clear distinction between [formally] automated systems and systems used in the pre-trial phase for "fact-checking". This implies, among other issues, that the court understands that the system is protected by the Intellectual Property Act, by not applying the exception of article 13 of Royal Legislative Decree 1/1996, of April 12, on intellectual property, which understands that the legal or regulatory provisions are not protected by intellectual property, and neither are the decisions of the courts and the acts, agreements, deliberations and opinions of public bodies. This provision is and interpreted in a literal and restrictive manner by the court, conversely as to the Civio Foundation, who for its part, understands that with BOSCO there is no such human intervention, since the granting of the social bonus in no case is verified by the Administration, but only, when necessary, by the electricity provider (the undertaking). According to Civio, Administration creates platform and the program, but subsequently does not carry out any other type of verification, so that, it is argued as being a functionally automated act.

However, Court understands that, not being an automated act, "Functional Analysis" provided originally by Ministry, which includes the technical specifications of the application, sufficiently allows to verify "how the computer system works and whether a given operation is correct, thus lacking allegation of the appellant regarding the existence of calculation errors in the application of solid basis". In addition, the court understands that, in this case, it applies the limit to transparency contained in article 14.1.k of the Transparency and Good Government Act, since it accepts as valid the report of the Ministry dated 4-12-2019 -supported by another report of the National Cryptological Center-, which argued that the delivery of the source code would make the application sensitive to attacks due to vulnerabilities that were to be discovered at the time the software product, and that could be used to access the databases connected to the application, which collect specially protected data, such as the disability or the status of victim of gender violence of the applicant.

ELECTRONIC NOTIFICATIONS

Tribunal Superior de Justicia de Madrid (Madrid Regional Court), case 212/2022, 5 May 2022, appeal number 535/2020

The citizen is responsible for the technical configuration of its devices for the use of the notifications website once it has been enabled.

Legal entities are required by Spanish law to communicate electronically with the Administration. The claimant in this case was PANIKER CONSULTORES, S.L, a legal entity to which the mandatory inclusion in the electronic notification mechanism was communicated. Therefore, from the date of receipt of this notification, the undertaking will be obliged to receive in the electronic enabled website all communications and notifications sent by Tax Agency.

Additionally, the Spanish law provides for the possibility of including a personal e-mail or phone number where a complementary notification, with mere informative purposes and no legal status, takes place. In this case, the claimant argues that due to an error that occurred within electronic site configuration, email was not recorded, and therefore he did not receive notice that he had a communication or notification in mailbox associated with your official electronic notification's site. Additionally, when the claimant tried to access notification site, it generated compatibility problems with browser and documents could not be read. This led to an extemporary administrative appeal that was rejected in the administrative proceeding.

In this judgement, Regional Court confirms the initial administrative decision for que following reasons: (1) the inclusion of the entity within electronic notification system implies a duty on the part of aforementioned entity to access electronic mailbox enabled for this purpose to check if any communication has been sent to it; (2) the applicant cannot allocate the responsibility for not having accessed its official electronic mailbox to the fact of not having received the notice in its personal e-mail, since such notice is not configured legally as necessary for the notification to be considered validly practiced (3) it is not justified in any way that the problems of access were attributable to the Administration, but they were instead due to configuration shortcoming of the browser (Google Chrome) of the appellant entity, being his responsibility to adapt the technical specifications to what is required

by the Administration.

The court makes it clear that only technical issues that are legally binding and attributable to the administration can result in the invalidity of the notification. Otherwise, we would be facing a certain carelessness or laxity on the part of the interested party, since it should have proceeded to check if it correctly accessed the official notification address.

TRANSPARENCY OF FACIAL RECOGNITION SYSTEMS

Consejo de Transparencia y Buen Gobierno CTBG (Transparencia and Good Governance Body), decision 665/2021, 18 February 2022, ref. 001-057088

Spanish law recognises right to access information about facial recognition systems being used by State Security Forces.

Claimant required to the Ministry of Interior information about each and every one of the places where the Civil Guard and / or any of the dependencies of the Ministry of Interior are testing or have tested technological facial recognition systems in any region of Spain, including the companies or entities that have provided the software for this purpose and/or with which they are collaborating.

The Secretary of State for Security denied, in accordance with articles 14.1.d) and e) of 19/2013 Act on Transparency and Good Governance, access to the information requested. Specifically, it was stated that the requested access may produce a real, and not merely hypothetical, damage to action of State Security Forces and Bodies in matters of public security and, related to this, jeopardize other initiatives for the prosecution and investigation of criminal offenders and, in particular, on the fight against terrorism and organized crime.

Appellant argued, on the contrary, that its request for access does not ask for specific information such as where exact geographical points the cameras may be located, but just general information; nor is required information about the identity of the people who are identified through these systems; nor other specific information related to the techniques being used, nor specific and technical information about how the Security Forces and Bodies carry out this surveillance task. The request was only meant to know whether they actually work with these systems and what they consist of.

In view of this background, the CTBG recalls that the possible application of certain legal limits to the information requested can only be considered in accordance with law if requirements of proportionality and express justification required are met. And in this sense, it proclaims generic and merely assertive nature of motivation given by Administration, which does not satisfy, even minimally, legal and judicial conditions and requirements necessary to consider application of a limit to right of access to public information to be well founded.

Furthermore, when it comes to the information requested on contracts concluded with private parties or other agreements, it should be borne in mind that Paragraph 8 of the 19/2013 Act on Transparency and Good Governance provides that, in general, this information must be the subject of active publicity, and therefore cannot be excluded from the right of access except in those aspects of the tenders which have been expressly classified as confidential.

Therefore, the CTBG obliges the Ministry to provide the required information on surveillance and facial recognition systems.

DATA PROTECTION AND REUSABILITY OF PUBLIC INFORMATION

Agencia Española de Protección de Datos AEPD (Spanish Agency for Data Protection), case PS/00204/2020, 6 May 2022

Obligation to specifically address the data subjects when processing public data collected from the public Administration.

The company EMÉRITA LEGAL undertakes activity consisting of the elaboration of profiles of lawyers and solicitors through processing of data from judgements published by the General Council of the Judiciary. The Committee for the Protection of General Council of Judiciary (CPDCGPJ), initiated appeal procedure before the AEPD for considering that the company was violating the GDPR.

Profiles that were elaborated included data such as name, surname, bar association, collegiate number, professional address, professional telephone number, professional email, number of cases defended, distribution of cases by areas of law, map of cases by court, etc. In addition, a ranking was made with lawyers with certain scores, as only data of “best” scored lawyers are published. AEPD notes that processing entails profiling, and therefore it is of application article 13 of GDPR, relating to principle of information, which requires, in paragraph 2 (f) controller to report on the existence of automated decisions, including profiling, referred to in Article 22,

paragraphs 1 and 4, and, at least in such cases, meaningful information on the logic applied, as well as the importance and expected consequences of such processing to the data subject.

In the first place, perspective is analyzed whether data treatment can be justified based on legitimate interest, as the company argued. According to the AEPD, and once all the types of interests, the necessity and nature of the treatment, the rights of those affected, the possible conflict of rights, and respect for essential content of data subjects have been delimited, in this specific case it considered that there is a substantial prevalence of legitimate interest and therefor treatment is lawful according to article 6 GDPR.

However, the requirements of Article 14 of the GDPR must also be complied with as regards information to be provided to data subject. At this point, defendant alleges that large number of affected people makes it disproportionate to address each and every one of those affected. The defendant explains in a general way for the public on its website the process of assigning IRJ and other points of the tool, but for collection purposes, data processing, exercise of rights and other mandatory aspects of article 14 of the RGPD, it does not do so, because on the web it is not addressed to professionals of the legal profession, neither mentions them nor contains the information elements expressed and unified in a clear and concrete way, in a specific section for those affected. Therefore, and considering the circumstances expressed in relation to the breach appreciated, from the point of view of the personal data protection regulations, the claimed entity is required to, within two months, adapt on its website to the personal data protection regulations the information offered to the lawyers and attorneys whose data are processed for the preparation of a ranking.

European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 209-213
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 17

Book Review

E. Psychogiopoulou and S. de la Sierra (eds.), *Digital Media Governance and Supranational Courts*, Edward Elgar Publishing, Cheltenham, 2022

This timely book collects and analyses relevant digital media cases at the supranational level in Europe, focusing on the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR). The book's overarching argument is that both supranational courts can significantly impact the applicable normative standards of digital media cases in a moment when the law regulating digital spaces remains uncertain. While the book includes an ambitious number of topics in the galaxy of digital media cases, the piece was able to deliver an understandable and comprehensive overview of how supranational courts can respond to challenges posed by digitalization. I believe the book should be on the shelves and laptops of scholars, lawyers, and policymakers considering that digitalization is and will transform all areas of our lives.

The book has 11 chapters that belong to two main parts. The first part is an analysis of cases from the CJEU, found in chapters 3 to 6. The second part is from chapters 7 to 10, in which the cases analyzed are from the ECtHR. The following lines are a summary of the findings of each chapter.

Chapters 1 and 2 serve as an introduction to the book. In the first chapter, both editors Evangelia Psychogiopoulou and Susana de la Sierra reflect on how new technologies are impacting our lives in unprecedented ways and how crucial legal questions and tensions between innovation and the protection of fundamental rights do not currently have a satisfactory regulatory response. As such, the editors and authors of the chapters base their arguments on the premise that European supranational courts have the potential to interpret norms to accommodate the novelties of the new digital ecosystem. In the second chapter, Susana de la Sierra makes the readers consider supranational courts as potential contributors to the process of regulating digital media to then introduce an issue regarding the very definition of digital media. Since there is a lack of a legal definition of digital media, courts are taking decisions without a clear background discerning between digital and traditional media. Despite this, however, De La Sierra argues that we should consider European courts and judges as valuable actors in the process of identifying and enforcing rights, freedoms, and obligations in the digital age. In addition to courts, the author argues in favor of a collaboration with independent authorities regarding digital media cases, considering that they have in-house experts that can deal with such technically challenging cases with the accuracy that is often needed to rule on these cases.

The following four chapters include an analysis of CJEU cases. Chapter 3 is about taxes in the digital space. In response to requests for the fair taxation of digital platforms and services, Begoña Pérez Bernabeu examines CJEU case law that deals with the taxation of the digital economy in light of worldwide and EU efforts to modernize the taxing system to reach intangible assets. She highlights the inadequacy of traditional tax policies for digital business models and the EU institutions' incapacity to pass legislation that is appropriate for the digital world. The compliance of the CJEU's progressive turnover-based company taxes imposed on digital intermediaries with EU legislation is then examined. The key conclusion made by Bernabeu is that the CJEU case law appears to have provided a remedy for the lack of EU legislation in the area of taxes by providing guidance on how to create national tax policies that are compliant with EU law. In Chapter 4, Valentina Golunova focuses on the duties that digital intermediaries have toward illicit content and explores the case law from the CJEU that clarifies them. The EU's intermediary liability scheme prohibits Member States from requiring digital intermediaries to continuously monitor user-generated content or aggressively look into allegations of criminal behavior. It appears that procedures that examine and revisit the boundaries of the prohibition on general monitoring have been sparked by technical solutions for automatic content filtering. According to the CJEU, online service providers may be required to execute a comprehensive removal of any content that is identical to or substantially similar to a particular piece of information that is deemed illegal. In order to evaluate the long-standing ban on widespread moni-

toring, Golunova investigates the interpretive actions taken by the EU judiciary. In Chapter 5, Federica Casarosa explores the CJEU's role in interpretation when working with national courts. She assesses the extent to which CJEU case law has impacted national data protection law, specifically the right to be forgotten. Casarosa finds that the CJEU introduces a novel interpretation in its landmark Google Spain case. Additionally, national courts employed unique interpretations and addressed the right to be forgotten from perspectives that the CJEU had not (yet) considered. The national courts respond to CJEU guidance in a variety of ways and can actually build on it, filling any gaps left by the EU judiciary, says Casarosa, demonstrating both the CJEU's potential to influence digital standards and its limitations. In Chapter 6, Evangelia Psychogiopoulou adds a different viewpoint to the discussion by examining the CJEU's role in interpretation, particularly with regard to fundamental rights in digital cases. This raises issues with how to interpret EU law, which itself aims to strengthen the protection of fundamental rights. In order to strike a fair balance between the fundamental rights and interests of creators and users, the EU copyright harmonization is known to have been built on two main pillars, one focusing on exclusive rights for authors and other creators and the other on exceptions and limitations to these rights. In light of the internalization of fundamental rights norms into EU copyright legislation by the EU institutions when establishing the appropriate rules, Psychogiopoulou examines the growing importance of fundamental rights analysis in the CJEU's interpretation of EU copyright law. The research by Psychogiopoulou demonstrates that the CJEU has occasionally creatively shaped and developed the legal norms specified in EU legislation by using fundamental rights.

The next four chapters deal with cases from the ECtHR. In his analysis of the ECtHR's rulings in an increasing number of cases involving digital media, Dirk Voorhoof in Chapter 7 makes a distinction between situations in which the ECtHR found that there had been a violation of Article 10 of the ECHR regarding freedom of expression and situations in which interference with online free speech was thought to be justified. The latter category addresses issues like the blocking of websites and social networking accounts, the identification of radical, extremist, or offensive content online, the integration of Internet archives, the (limited) liability of online platforms for user-generated content and hyperlinks, and the safety of journalists' sources in cyberspace. In his analysis of the ECtHR's rulings in an increasing number of cases involving digital media, Dirk Voorhoof makes a distinction between situations in which the ECtHR found that there had been a violation of Article 10 of the ECHR regarding freedom of expression and situations in which interference with online free speech was thought to be justified. The latter category addresses issues like the blocking of websites and social networking accounts, the identification of radical, extremist, or offensive content online, the integration of Internet archives, the (limited) liability of online platforms for user-generated content and hyperlinks, and the safety of journalists' sources in cyberspace. Through Chapter 8, Kristina Cendic and Gergely Gosztonyi show how the ECtHR's jurisprudence has undergone new dynamics as a result of the changes brought about by new technologies and the Internet to the concept of "public watchdogs." By focusing on the fuzziness of the definition of media, they examine the rising number of applications filed with the ECtHR by a wider spectrum of actors who aim to hold authority accountable and analyze pertinent ECtHR case law. They concentrate on cases that deal with specific facets of the right to information, particularly the right to receive information, considering, for example, situations when state interference takes the form of banning or limiting Internet access. Additionally, they look at cases that explore the obligations that states parties to the ECHR have in terms of access to information and data held by public authorities. These are important issues because they affect how (digital) media and other information agents operate and how a democracy's public discourse is facilitated. They emphasize the importance of new players, such as bloggers or non-governmental organizations, as well as new technology, like mobile applications, for this goal, which creates a new environment for basic rights discussion. In Chapter 9, Gloria González Fuster focuses on the ECtHR's capacity to provide fresh perspectives to the interpretation of earlier legal precedents in order to address particular issues posed by the digital revolution. The focus is on how the ECtHR addresses the issue of online gender-based violence, a significant social issue that is still barely handled by law and policy. The ECtHR has taken a helpful approach to the problem by drawing parallels between domestic violence and cybercrime, acknowledging that cybercrime can

take many different forms, such as the collection, sharing, and manipulation of data and images, as well as digital invasions of privacy and access to the victim's computer. The ECtHR has also reaffirmed that states subject to the ECHR have a positive obligation to set up and rigorously enforce a system that criminalizes all types of domestic violence, whether it takes place offline or online, and to adequately protect the victims. However, the ECtHR has made decisions in circumstances of gender-based online violence unrelated to domestic violence when it has neglected to take the "gender" dimension into account. This, according to Fuster, emphasizes the necessity of adopting a broader perspective on online gender-based violence and addressing the subject in all of its complexity. Disinformation is not a new phenomenon, according to Iva Nenadic and Verza Sofia in Chapter 10, but it has taken on a new dimension as a result of the growing usage of digital media. The authors emphasize how spreading false information about illnesses and treatments may have an adverse effect on a variety of rights, including the freedom of information, and how it may even endanger people's health. In light of this, nations and supranational organizations, such as the EU, have adopted a variety of disinformation-fighting tactics, and in certain cases, courts have been asked to rule on whether particular rules are compatible with fundamental rights. The ECtHR and the CJEU are both in a position to evaluate this compatibility, and by doing so, they contribute to defining the legal framework in which nations may act in response to disinformation. Nenadic and Verza demonstrate the active role of courts as participants in the process of digital media governance from this specific perspective by providing a thorough assessment of the ECtHR's case law in this area.

The last Chapter serves as a conclusion. In Chapter 11, the CJEU and the ECtHR's contributions to the creation of legal norms governing digital media and the Internet are summarized by Domenico Rosani and Clara Rauchegger. They not only summarize the main findings but also offer an analysis that helps frame the constitutional issues with digital media in Europe from the standpoint of fundamental rights. They emphasize the conflicts that exist between rights and liberties and talk about how European supranational courts are handling these conflicts and determining the legislation that will apply. They highlight the advantages of digitization in this context, particularly in terms of freedom of speech and information, but they also discuss how harm can be done to people and how courts are providing protection in this regard. In opposition to this paradigm, they advocate for states to have a more active role in explicitly defining both rights and obligations. Additionally, they argue against changing the essence of the judiciary by giving it a particularly wide range of appreciation, which would in practice turn it into a legislator, while highlighting the importance of judicial adjudication.

Digital Media Governance and Supranational Courts is an important read not only because he way in which digital media cases are approached is a comprehensive one, but also because the findings of the book allow it to become a crucial piece of the puzzle of literature on digitalization (reviewed by INÉS JIMÉNEZ MARTÍNEZ).

E.Mª Menéndez Sebastián and J. Ballina Díaz, *Sostenibilidad social y ciudadanía administrativa digital*, Reus, Madrid, 2022

This In recent years, we have witnessed a deep change in the relationship between public authorities and society. This book shapes it from a new, dual, perspective: citizenship and social sustainability.

Social sustainability, as defined by the European Economic and Social Committee, is the capacity to guarantee the conditions necessary for human well-being (security, health, education, democracy, participation and justice) equally distributed between classes and genders, and its ultimate objective is to reduce inequalities. 2030 Agenda for Sustainable Development and its seventeen goals represent the horizon within which to make innovation and sustainable development compatible by linking global and national initiatives.

The book is divided in two sections. The first one is aimed at answering the question of what citizenship is today; the second part carries out an in-depth study of the new public governance and its effects in the way Administration and citizens relate to each other, as this study focuses on the relationship between citizens and public authorities, in one of them, the Public Administration.

The authors begin by reflecting on what it means to be a citizen today, unpacking those elements that are essential, such as the idea of a common project, commitment and equality. This last aspect connects the subject again with sustainable development, in the sense of achieving

the goal of reducing inequalities, an idea that is also present in the analysis of the new public governance.

Then, the authors analyse the change from democratic administration to administrative democracy and how this has transformed the relationship between Public Administration and citizens, who are no more administered or users, but citizens *of* and *in* the Administration. To do so, they import the French notion of administrative citizenship, which the authors also connect with the idea of good administration.

Going a step further, they offer as well a perspective on digital citizenship, given that another fundamental aspect in this relationship is technological disruption, which offers great opportunities for the realisation of this renewed citizenship, but also conceals potential risks, such as digital divide or algorithmic discrimination, which could attack equality head-on, an essential element of the very notion of citizenship. Nor do they forget to mention some new forms of guaranteeing these new rights that the notions of administrative citizenship and good administration protect, such as the figure of the Ombudsman.

Once this new relationship between the Public Administration and citizens has been set out, the second part of the book moves on to study another current concept: public governance. The authors examine how all the new notions introduced in the first chapter should be reflected in the day-to-day workings of Administration. They consider seven key points in order to achieve what they believe should be the objective of Public Administration, i.e. comprehensive, innovative, effective, efficient and inclusive public management.

In this way, the book offers not only a theoretical study but also a roadmap for Public Administrations and citizens, to understand both the reasons for the new situation and the consequences it entails. Thus, it emphasises the multiplicity of aspects involved in public decision-making.

The authors study public ethics as a basic prerequisite for regaining the trust of citizens, devoting specific attention to codes of conduct, as a *tertium genus* between the ethical and the legal, transparency and open data. Another essential element of this new governance is undoubtedly participation, as it contributes to a greater legitimisation of administrative power, which facilitates the acceptance of decisions and contributes to greater efficiency. Particular importance is attached to accountability and, especially, to evaluation in the improvement of decisions. While these principles are common to both good governance and good administration, the authors point out the differences that exist among those areas, as political decisions are not the same as, for instance, public services management. Different essential aspects of public management are also considered, such as effectiveness and efficiency, which are vital to achieve good administration; innovation, especially people-based design or the co-creation of public services; and, of course, equality, the backbone of the system.

As the authors conclude in their book, inspired in quality, reflection and the spirit of improving things, we are witnessing a real disruption in our society, mainly derived from two different but converging fronts: new relationship between citizens and public authorities, in particular the Administration, and digital transformation.

Within the first aspect, the French idea of administrative citizenship stands out, together with that of political citizenship. It reflects very accurately the parameters of what could be called the right of all to participate not only in political life, but also in administrative life and in the decision-making processes implemented at this level. This connects unfailingly with the notion of good administration, which contributes to better decision-making. By implementing the notion of administrative citizenship, Public Administration will be able to answer to social demands more properly and with greater legitimacy. Therefore, a better acceptance of the administrative decisions themselves will be achieved.

The new public management model of public governance, which hinges on key principles such as public ethics, transparency, participation, accountability, effectiveness and efficiency, innovation and, above all, equality, also responds to this. Equality is also the ultimate goal of social sustainability.

Finally, the digital revolution contributes to the effective realisation of this renewed citizenship, offering new tools that ease its exercise, although not without significant risks, such as the digital divide or algorithmic discrimination. Hence the need to integrate the principle of equality in a transversal way, to implement the new instruments and tools of public governance with all the guarantees and in favour of making the aforementioned sustainable development effective, while complying with several of the goals set by 2030 Agenda.

In short, we are facing a time of change that need to be faced correctly. Public Administration and Government cannot lag behind in order to achieve sustainable social development, essential in a society that seeks a common project. Prof. Menéndez Sebastián and Ballina Díaz contribute to this objective by doing their bit through their study. A perfect starting point for further steps on scholar academia. (reviewed by ALEJANDRA BOTO ÀLVAREZ).

Classificazione Decimale Dewey:

340.0285 (23.) DIRITTO. ELABORAZIONE DEI DATI

Printed in July 2023
by «The Factory S.r.l.»
00156 Roma – via Tiburtina, 912

ISSN 2724-5969

ISBN 979-12-218-0078-4

30,00 EURO