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

*Data and Digital Sovereignty**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. *The European legislation*

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

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

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

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

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

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

[5] See p. 1 of the Memorandum.

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

[7] See p. 7 of the Memorandum.

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

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

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

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

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

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

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

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

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

themselves within the "new spaces".

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

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

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

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

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

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

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

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

This has come as a shock for public authorities.

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

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

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

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

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

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

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

4. *Conclusions*

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

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

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

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

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

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

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

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

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

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

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

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

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