ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 5, No. 3, 270-274 (2020)
www.astesj.com

ASTES Journal
ISSN: 2415-6698

Digital Sovereignty Between "Accountability" and the Value of Personal Data

Nicola Fabiano[*,1,2]

[1]*Studio Legale Fabiano, 00179, Italy*

[2]*International Institute of Informatics and Systemics (IIIS), 34787, Florida, USA*

ARTICLE INFO

Article history:
Received: 03 April, 2020
Accepted: 18 May, 2020
Online: 28 May, 2020

Keywords:
Digital sovereignty
Data Protection
Privacy
Ethics

ABSTRACT

In the last year, especially in Europe, the expression "digital sovereignty" has been used very frequently to describe, above all, the primacy of a State. Indeed, the "digital sovereignty" is a complex concept, which entails cross-reference with several sectors and contexts. We believe that the concept of "digital sovereignty" can be two sides of a coin. On the one hand, we can use the expression "digital sovereignty" to describe the supremacy and full control of a State on the digital area. On the other hand, we can use the same expression "digital sovereignty" to refer to the power on the digital domain - as we will explain in our contribution - that anyone is potentially able to use in the private or public sector. Our contribution aims to demonstrate that where someone, public or private, can have the control on the digital domain, there is "digital sovereignty".

1 Premise

Digital sovereignty has multidisciplinary connotations, and it can assume different meaning or describe several aspects depending on the contest in which we refer to it. We would demonstrate how it is possible to find other "digital sovereignty" scenarios different from the traditional description of the digital power that a State uses to protect its cyberspace borders.

We aim not to deepen here on the entire digital sovereignty topic but, starting from the definition of both the terms "digital" and "sovereignty", we demonstrate how it is possible to realise a "digital sovereignty" also by a private organisation and not only by States.

Furthermore, we analyse what are "digital sovereignty" impacts on data protection and privacy, highlighting the consequent effects and possible approaches.

We think that there is undoubtedly existing "digital sovereignty" also in the private sector, which is expressed mainly through the adopted internal approach on the digital by some organisations that have relevant effects outside them indeed.

Indeed, starting from the analysis of "digital sovereignty" traditional concept, we would highlight how is preeminent nowadays, the digital aspect in any contest and how private organisations carry it out.

2 The meaning of "sovereignty"

The purpose of this contribution, as we said, is to investigate looking for an adequate definition, starting from the terms "digital" and "sovereignty" and analysing the meaning of both single words, till the expression "digital sovereignty" and so to have a proposal of complete definition.

The sovereignty topic is not recent and anyway related to the description of nature and characteristics of a State. Indeed, we can find many references to the sovereignty in the juridical literature about the study of a State. We bypass to deepen the traditional sovereignty concept because it is well-known.

3 The meaning of "digital"

For some time, there have been casual use of the word "digital" (in a sense opposed to "analogic"), with which commonly reference made to the possibility of representing information in the form of numbers.

The word "digital" derives from the Latin "digitus" (finger) because the ancient Romans used fingers to count. Nowadays, the term "digital" - among other definitions - refers in general to the number system. And specifically to the binary number system (0 or 1, off or on) on which a computer is based. With the spread of new technologies and, hence, with the use of techniques or algorithms

[*]Corresponding Author Nicola Fabiano - info@fabiano.law

based on numbers or binary system, became common to refer to the term "digital".

In the most common and widespread language, it is customary to intercept the word "digital" when it is used to describe, with a non-technical approach, only the use of a device (smartphone, tablet, computer) and/or the Internet. In general, the digital term represents, in the collective imagination, a general sense of innovation in its most heterogeneous manifestations and applications.

Hence, what is digital?

We reach a conventional definition, even if not nearly deep, broad or basic enough [1], according to which digital is synonymous with a set of electronic computing techniques[1].

4 What do we mean by "Digital sovereignty"?

In light of the synthetically described panorama, it would emerge a definition of "digital sovereignty" as the power expressed in an innovative context.

In summary, therefore, we would affirm that with the expression "digital sovereignty" we intend to refer to the power attributed to the State in the sphere that concerns any activity classifiable as "digital", that is connected to the use of the technologies or derived from them.

The outcome of a brief survey on international scientific production related to the topic, aimed at considering whether there is a theoretical convergence in the qualification of digital sovereignty, has produced thought-provoking results.

Among the most recent publications, Couture [2] claim that the expression "digital sovereignty" is characterized by five different perspectives ("*Cyberspace Sovereignty*", "*Digital Sovereignty, Governments and States*", "*Indigenous Digital Sovereignty*", "*Social Movements and Digital Sovereignty*" and "*Personal Digital Sovereignty*"). Not wanting to go into detail, the constant reference to the digital term proposed by Peters [1] emerges, namely a generic and conventional definition based on the calculation.

It would seem that only in the nineties was the term digital super-gravity introduced [3, 4], used to envisage the internet as an opportunity to exercise independence from state control.

However, especially in recent times and more increasingly, we assist in the spreading of the use of the expression "digital sovereignty" to refer to the extraordinary power of a State, particularly in the digital domain.

This approach has drawn some attention limited to describing a phenomenon related to cyberspace, and specifically to the power of a State regarding its digital borders.

Digital sovereignty, moreover, has aroused the interest of Data Protection Authorities by aiming to investigate what kind of impact it would have on the protection of personal data. In fact, "digital sovereignty" was the topic of the event organised by the Italian Privacy Data Protection Authority (DPA) on the occasion of the Data Protection Day (Rome - 29/1/2019)[2].

It is well-known that with the term "sovereignty," we generally refer to a power (of State, of people, of economy, etc.), original and independent from any other, and expressed by the manifestation of a will.

The different definitions of "digital sovereignty" have in common only the meaning to express primacy on something but not on the digital domain in a broad sense; the technology's primary role, whose development or diffusion involves the manifestation of power anyway, might be "digital sovereignty."

The primary reference is to the technological scenario which sees a current fierce competition between the USA, China, and Europe, hoping from this latter an effective intervention [5] to improve technological development and counter the supremacy of other countries.

We have the impression that with these positions, there is the aim at soliciting European development policies that are adequate to support confrontation with other states rather than aimed at the expression of power over a domain. In essence, increasing competitiveness in Europe, it implies an improvement both in the internal and in the global market: sovereignty, therefore, would express as supremacy on the market. Some people have doubts about whether this is a case of protectionism [6].

Furthermore, there is a widespread fear of losing control over technologies, both at the national and European or international level; there are different resources on the Internet. Moreover, Ursula von der Leyen, President of the European Commission, in the document entitled "**My agenda for Europe**", states, "*It may be too late to replicate hyperscalers, but it is not too late to achieve technological sovereignty in some critical technology areas*".

We can find a lot of news, already published, that express the same concern. Among several contributions, we highlight the article entitled "Digital sovereignty does not need EU champions" published on 14 November 2019, in the Financial Times where we read: "Building an ecosystem of services which protect user data would fill a neglected niche between the corporate wild west of the US and the state panopticon of China. Its appeal would not be restricted to Europe, either." The positions highlighted, in summary, can be considered concurrent, since the common denominator is constituted by a widespread desire not to allow the big five tech companies - GAFAM - to process the personal data of European citizens. Fear, market, and technological supremacy converge towards the need for greater security for personal data.

4.1 Digital sovereignty and cyberspace

The reference to the power of the State over the digital domain has led to limiting the scope of this power to cyberspace, so that, for example, in Italy the recent Legislative Decree no. 105/2019, converted with modifications by the Law 18 November 2019, n. 133, on "*Urgent provisions on cybernetic national security perimeter and discipline of special powers in sectors of strategic importance*", with article 1, paragraph 1, institutes the "cybernetic national security perimeter". This recent legislative innovation, which undoubtedly deserves further study, has led to the affirmation of digital

[1] The author says "That conventional sensein which digital is synonymous with discrete electronic computing techniquesis not nearly deep, broad, or basic enough."

[2] Here: `https://www.garanteprivacy.it/documents/10160/0/I+confini+del+digitale.+Nuovi+scenari+per+la+protezione+dei+dati+-+Atti+del+Convegno.pdf/89efdb61-c0c3-cc6f-8037-f0b283bad2b4?version=1.0`, last access May 2020

sovereignty understood as the power of the State over cyberspace.

However, recently, Roguski [7] affirmed that we are facing "layered sovereignty in cyberspace" approach. The author identified logical and social layers of cyberspace that "may be open to the exercise of State authority based on a criterion of proximity, i.e. whenever the State can establish a genuine link with the digital objects or online personae over which authority is to be asserted".

In our opinion, in relation also to what we referred to, it is possible to identify further profiles of the exercise of digital sovereignty that need not necessarily be taken over or dominated by the State.

Moreover, Couture [2] states that the notion of sovereignty in the world of digital "is increasingly used to describe various forms of independence, control, and autonomy over digital infrastructures, technologies, and data". not necessarily state and "meanings, and definitions of sovereignty can significantly differ from one group to another."

These authors, having registered as a common denominator of technological sovereignty (of which the digital one is a part) autonomy, independence and control, conclude their research with the following question: "unsettling digital sovereignty?" [2].

This statement should make people think.

4.2 Digital sovereignty: proposal for a definition

In any case, in light of this, it is possible to affirm that "digital sovereignty" - in general terms - is not exclusively identified with the power exercised by the State.

In fact, "digital sovereignty" can be expressed in any model adopted by the private sector through which the power over one's digital domain is exercised (in autonomy and with full control). This power may correspond to actions undertaken, to choices of particular work technologies, and hence, to the intention of preserving the digital heritage.

Thus, we can define "digital sovereignty" as the power over one's digital domain exercised by a State's or even a private organisation one. The key-point is related to the "power over ones' digital domain". In the case of a State, that power will consist of any activities aimed to protect its cyberspace. A private organisation may exercise that power carrying out any activity focused on the own digital domain (protect, develop, spread, propose, sell, etc.). Ultimately, we can have different "digital sovereignty" approaches depending on the (private or public) bodies. It is not a matter of subjective profile, but the main point is the power and how it is exercised.

We agree with Roguski [7] - although he refers to a different field - regarding a concept of layered "digital sovereignty", depending on the specific area (public, private, etc.). It may be the likelihood of being in front of different kinds of "digital sovereignty".

This approach, undoubtedly, also significantly affects the aspects related to the protection of personal data in the exercise of digital sovereignty.

5 Digital Sovereignty and Inclusion

Digital sovereignty, besides, should also be characterized by an inclusion process of individuals fundamental rights in their domain, and thus avoid to be confined outside the protection of personal data.

So far, the phenomenon of digital sovereignty has been described as power over a domain.

Nevertheless, apart from the definition as described before, digital sovereignty is so versatile that it cannot be ruled out that it may also constitute the opportunity for one or more individuals to acquire digital autonomy and sovereignty. In this direction, to increase the knowledge of individuals, sovereignties could be enriched by awareness campaigns and in this way, obtain added value.

In fact, according to Nitot [8], awareness is an integral part of what means technological sovereignty. The (perfect) awareness of the current digital condition of the user will favourably affect his choices also regarding technologies and his personal data.

The data subject, that be aware, will be able to decide, by exercising his power of self-determination, even in the context of digital sovereignty. That decision is not by merely refusing the technologies, but by implementing appropriate choices aimed at avoiding the expropriation (in part or all) of his data personal, losing control over them.

According to Nitot [8], the "privacy by design" principle[3] is precisely in this sense, as it is the tool to induce the user to increase his awareness to acquire the necessary tools to defend himself.

6 Digital Sovereignty: the Limits

The most crucial matter is if "digital sovereignty" can be a limit for privacy and data protection.

Digital sovereignty in its layers or different perspectives, qualifying as a power over the digital domain, cannot, however, constitute a limit, intended as pre-eminence on the individual and his rights, especially those related to the protection of personal data.

Indeed, the only limits are those provided for by the law and, concerning the digital sovereignty and specifically to the sovereignty over cyberspace, it is evident that the law on the protection of personal data does not apply in cases of national security.

Moreover, this is expressly envisaged by the recital nr. 16[4], as well as Articles 2 and 23 of the EU Regulation 2016/679 (GDPR) [9].

7 Digital Sovereignty and the Rules on the Protection of Personal Data

The EU Regulation 2016/679, General Data Protection Regulation (GDPR) regulates the protection of natural persons and places the data subject, the person who has the power over their data, at the centre of the entire system, of the processing. Technological evolution does not mean abuse his (its or her) power on the individual but

[3] lay down by Article 25 of the EU Regulation n. 2016/679 - GDPR

[4] (16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

ensuring a necessary balance between innovation and protection of humans. In the current globalised system that leads to the acquisition of an overall and non-analytical view, it is needed to refer to a general legal framework[5] [10] of principles regarding privacy and protection of personal data that is widely valid. An instrument is already available today: the Convention 108+ and one can proceed from the principles outlined in it.

Personal data is an absolute value because it belongs to any natural person and it is inevitably and ontologically linked to it. Furthermore, personal data contribute to characterising the primacy of human dignity from which one cannot ignore and even clumsily try to disqualify by treating such information as if it were a secondary aspect of the person.

As already stated in another contribution [11], the protection of personal data and privacy are discussed solely and exclusively as there are ad hoc regulations; otherwise, there would be no problem of dwelling on the essence and relevance of personal data.

We cannot overlook, however, that personal data must be considered as an absolute value, also through an ethical approach and in any case, regardless of any norm [12].

The preventive criterion based on the principle according to which the personal data is an absolute value and requires awareness and ethics must be considered as a "prerequisite": this constitutes the true and real starting point, not codified, which stands as an ultra-legal element [13].

The "level zero", the right starting point, is also the ethical consideration of the high value attributable to personal data; without this assumption, it is difficult to have a suitable approach to the law. The "level one" will be that of legal rules.

8 Digital Sovereignty and Accountability: a Possible Challenge

The data controller must comply with the principle of "accountability" as required by art. 5, paragraph 2, of the GDPR. We should not attribute to this concept merely a legal meaning, because it is laid down by the GDPR, but also a programmatic nature. In fact, in qualifying the accountability and, therefore, considering the data controller as accountable, it should be necessary an assessment of the organisational measures to be implemented. In this way, the controller, respecting of every available instrument (good practice, guidelines, standards, etc.), minimises risks and protects the personal information belonging to the individual.

We should add to this not only the respect for ethics but also, equally, the development of a genuinely ethical conscience; if we apply ethics together with the juridical norms, we could connote the principles enunciated by the Convention 108+ and the GDPR in concrete.

It is no coincidence that the 41st International Conference of Data Protection and Privacy Commissioners, held in Tirana in October 2019, has adopted the "*International resolution on privacy as a fundamental human right and a precondition for the exercise of other fundamental rights*"[6] where we read the following, explicit statement: "**Reaffirm a strong commitment to privacy as well as to right and value in itself, given various international obligations**".

In conclusion, the principle of accountability appears to be compatible with public or private digital sovereignty, where the primary reference value remains the natural person and human dignity. Digital sovereignty that is in contrast with respect for human dignity is not acceptable.

9 Conclusions

Digital sovereignty is a broad concept which can refer to the national security but also to the (digital) power expressed by someone (company or organisation or Public Body). Thus, we believe that nowadays, it is possible to discuss in terms of "sovereignty" related to anyone public or private ones. By this approach, it is evident that any case or situation deserves appropriate evaluation to verify whether we are dealing with a hypothesis of "digital sovereignty".

References

[1] B. Peters, Digital Keywords - A Vocabulary of Information Society and Culture, Princeton University Press Princeton and Oxford, 2016, 94, http://culturedigitally.org/wp-content/uploads/2016/07/Peters-2016-Digital-Digital-Keywords-Peters-ed.pdf [retrieved: May, 2020]

[2] S. Couture - S. Toupin, What does the notion of "sovereignty" mean when referring to the digital?, 2019, New Media & Society, 21(10), pp. 23052322. doi: 10.1177/1461444819865984.

[3] J. Perry Barlow, A Declaration of the Independence of Cyberspace, 1996, Electronic Frontier Foundation - https://www.eff.org/fr/cyberspace-independence [retrieved: May, 2020];

[4] F. Turner, From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism, 2006, Chicago, University of Chicago Press.

[5] ENISA - Consultation paper - EU ICT Industrial Policy: breaking the cycle of failure, July 2019, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper [retrieved: May, 2020]

[6] European 'tech sovereignty' or 'tech protectionism'?, 30/10/2019, http://www.project-disco.org/european-union/103019-european-tech-sovereignty-or-tech-protectionism/ [retrieved: May, 2020]

[7] P. Roguski, Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment, [in:] T. Minrik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (eds.), 11th International Conference on Cyber Conflict: Silent Battle, 2019, p. 347-359.

[8] T. Nitot, Numrique: reprendre le contrle, Paris: Framasoft, 2016, 15. https://framabook.org/docs/NRC/NumeriqueReprendreLeControleCC-Byimpress.pdf [retrieved: May, 2020].

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [retrieved: May, 2020]

[10] N. Fabiano, Privacy and Security in the Internet of Things, in Cutter IT Journal, Vol. 26, No. 8, August 2013.

[5] We proposed this approach in the contribution entitled "Privacy and Security in the Internet of Things" published by Cutter IT Journal8 (Vol. 26, No. 8 August 2013); see references.

[6] http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf [retrieved: May, 2020].

[11] N. Fabiano, Protezione dei dati personali e privacy: qual lo starting-point?, 2019, https://www.nicfab.it/protezione-dei-dati-personali-privacy-qual-lo-starting-point/ [retrieved: May, 2020].

[12] Charter of Fundamental Rights of the European Union, 2016 https://www.ecb.europa.eu/ecb/legal/pdf/oj_c_2016_202_full_en_txt.pdf [retrieved: May, 2020]

[13] The Treaty on the functioning of the European Union (2016/C 202/01), 2016. https://www.ecb.europa.eu/ecb/legal/pdf/oj_c_2016_202_full_en_txt.pdf [retrieved: May, 2020]