REVISTA DIREITO MACKENZIE

ISSN: 23172622

DATA STORAGE AND DIGITAL SOVEREIGNTY. A REINTERPRETATION OF PUBLIC (BIG) DATA GOVERNANCE IN THE LIGHT OF NEW GLOBAL CHALLENGES

Valentina Pagnanelli*

RECEBIDO EM:	23.3.2022
APROVADO EM:	4.4.2022

* PhD scholarship University of Florence. PhD student in Legal Sciences at the University of Florence, lawyer, data protection consultant. E-mail: valentina.pagnanelli@unifi.it

2022 | v. 16 | n. 1 | p. 1-32 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v16n115229

ABSTRACT: Using data retention policies in the public sector as a paradigm, the paper reflects how States assert or defend their digital sovereignty. The article recalls the digitization path of the Italian PA, on which big data has had a significant impact. Digital data storage has imposed the transition from paper archives to the cloud, a transition regulated by national and European legislation and partly influenced by the digital strategies of the great world powers. The proliferation of localization obligations and prohibitions confirms the complexity and centrality of these issues in protecting digital sovereignty. The paper ends with an analysis of the key points of the European strategy for data published by the European Commission in February 2020 and with a look at the Franco-German data storage and data sharing project called GAIA-X.

KEYWORDS: Data storage; digital sovereignty; public sector; data localization.

ARMAZENAMENTO DE DADOS E SOBERANIA DIGITAL. UMA REINTERPRETAÇÃO DA GOVERNANÇA PÚBLICA (BIG) DE DADOS À LUZ DE NOVOS DESAFIOS GLOBAIS

RESUMO: Utilizando como paradigma as políticas de retenção de dados no setor público, o artigo reflete sobre como os Estados estão afirmando ou defendendo sua soberania digital. O artigo relembra o caminho da digitalização da AP italiana, na qual a big data teve um impacto significativo. O armazenamento digital de dados impôs a transição dos arquivos em papel para a nuvem, uma transição regulada pela legislação nacional e europeia e parcialmente influenciada pelas estratégias digitais das grandes potências mundiais. A proliferação de obrigações e proibições de localização confirma a complexidade e centralidade dessas questões na proteção da soberania digital. O artigo termina com uma análise dos pontos-chave da estratégia europeia de dados publicada pela Comissão Europeia em fevereiro de 2020 e com uma análise do projeto franco-alemão de armazenamento e compartilhamento de dados chamado GAIA-X.

PALAVRAS-CHAVE: Armazenamento de dados; soberania digital; setor público; localização de dados.

1. Introduction

On 24 April 2020, The Guardian ran an article with the headline: "*UK government told not to use Zoom because of China fears*[1]". The article noted that "*Government and parliament were told by the intelligence agencies last week not to use the videoconferencing service Zoom for confidential business, due to fears it could be vulnerable to Chinese surveillance*".

The National Cyber Security Centre had reportedly advised members of the UK government and parliament against using the Zoom video conferencing platform[2], at least for meetings classified as "confidential"[3].

***

On 29 October 2019, the GAIA-X project was presented during the annual German Digital Summit. This was a fully European cloud infrastructure, interoperable and independent from services provided by the US and Chinese providers. Chancellor Angela Merkel, on that occasion, stressed the importance of finding European solutions to guarantee data sovereignty[4]. The Franco-German project[5] proposes the implementation of a system as an alternative to the services offered by the cloud giants, which would ensure compliance with high ethical and security standards and be based on the principle of *data sovereignty by design*, in order to create a common European space for data storage[6].

***

1 The article is available at this link https://www.theguardian.com/uk-news/2020/apr/24/uk-government-told-not-to-use-zoom-because-of-china-fears.

2 This tool became hugely popular due to social isolation and distancing measures introduced to counter the Covid-19 pandemic. The main theme of this research is not strictly related to the pandemic. However, the paper will repeatedly refer to acts, documents, and decisions related to the pandemic itself, assuming that the context of the global health emergency declared by the World Health Organisation on 30 January 2020 is known to readers.

3 As early as the beginning of April, a research center at the University of Toronto had already highlighted the weaknesses of the encryption system used by the platform and the risks arising from the fact that the security keys provided to participants in Zoom meetings were sent from servers located in China: "*An app with easily-identifiable limitations in cryptography, security issues, and offshore servers located in China which handle meeting keys presents a clear target to reasonably well-resourced nation-state attackers, including the People's Republic of China*" (MARKZAR; SCOTT-RAILTON, 2020).

4 See https://www.bundesregierung.de/breg-en/search/kanzlerin-bei-digitalgipfel-1686546.

5 The common position of 18 February 2020 is available at this link https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10.

6 The project was officially presented on 4 June 2020 at an event sponsored by the *German Federal Ministry for Economic Affairs and Energy*.

2022 | v. 16 | n. 1 | p. 1-32 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v16n115229

On 7 April 2020, in its initial comments on the Covid-19 contact tracing app under consideration by the "data-driven"[7] working group set up by the Government, the Italian Data Protection Authority drew attention to the need for a judicious choice of technological partners, given the high risk involved in processing citizens' data. The Data Protection Authority also recommended giving preference to entities "*located on Italian territory*[8]". In an interview published in Cybersecurity Trends on 16 April 2020, the President of the Data Protection Authority again addressed the subject, highlighting a clear need to rethink public governance to protect the digital sovereignty of the State in the face of growing global threats to the independence of countries: "*In a 'dephysicalised' space like the network, sovereignty must exist in new forms, governed less by the traditional criterion of territoriality and more by the capacity of States to protect rights effectively and the democratic form itself [...]*[9]".

***

"*Territory, sovereignty, and power are the burning issues in Internet law, and have to be addressed*" (POLLICINO, 2019). This was how Oreste Pollicino eloquently introduced his commentary on two judgments of the European Court of Justice[10]. The Luxembourg judges were called upon to rule on establishing territorial limits to the application of European law, arrived at apparently contrary solutions[11].

Even this brief and limited review shows that although the abovementioned constitutional categories require rethinking, they remain essential for governing the global digitalised context of our times.

Using public sector data storage and access policies as a paradigm, this paper discusses how States are asserting their digital sovereignty. This is in a historical phase in

7 Italian Data Protection Authority, *Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro data-driven per l'emergenza COVID-19*, 7 April 2020, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316821.

8 This request was fulfilled in Article 6 of Decree-Law 28/2020, which specifies that the single national platform managing the prospective alert system will be implemented "*exclusively with infrastructures located on national territory*".

9 The full text of the interview can be found at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9317569.

10 The decisions in question were: Court of Justice of the European Union, judgment C-507/17, Google LLC v Commission Nationale de l'informatique et des libertés (CNIL), 24 September 2019; Court of Justice of the European Union, judgment. C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Limited, 3 October 2019.

11 For an analysis of the two cases, see POLLICINO O., "*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*", cit.

which, on the one hand, the territory becomes the go-to yet carelessly used reference to identify and protect the boundaries of an increasingly intangible jurisdiction. On the other hand, democratic systems and citizens' freedoms and rights are threatened by the increasing and pervasive use of artificial intelligence[12].

2. From digitalisation to big data: the new public sector playing field

We will not go over the stages of recent technological growth, which has systematically taken us from paper to digital in a few years. The current scenario in which Big Data and, in particular, Big Data Analytics have effectively changed man's relationship with information[13].

A crucial component of this evolution is certainly the progressive digitalisation of public administrations' information assets, which has led to the constant updating of PA databases[14] containing extraordinary amounts of information, be it personal data, special categories of data, or non-personal data[15]. The Italian Public Administration (PA), which we will focus on in the first part of the discussion, has not been left out of this paradigm shift.

Indeed, following the decisive boost to the digitisation of public administrations, in particular with Decree Law 179/2012, which led to the gradual creation, among others, of the National Register of Residents, the electronic student file, and the electronic health file (set up by the Regions and autonomous provinces), the Italian Public Administration has taken on "*the responsibility of managing, processing, sharing and elaborating huge 'digital archives' from which information may be taken that could compromise both national interests and individual rights*" (CALZOLAIO, 2016, p. 198).

12 "*If we hold on to a tradition [...] whereby law is a fact, the fact of the will of the strong, and we continue to base it on sovereignty, we will have a hard time understanding and governing a present in which sovereignty can be defeated (to give but one example) by an intelligent, computer-savvy youngster. [...] We were used to thinking for two hundred years that sovereignty was the basis of law. Let us now try to think of law as the basis of sovereignty*" (GENTILI, 2011, p. 205).

13 For an effective description of the risks and potential of Big Data analytics, see CALZOLAIO S., *Protezione dei dati personali*, aggiornamento, in Digesto delle discipline pubblicistiche, UTET, Turin, 2107, pp. 594 ff; on Big Data and machine learning, SIMONCINI A., SUWEIS S., *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in Rivista di filosofia del diritto, I, June 2019, pp. 87-106.

14 We need only look at the Databases of national interest list in Article 60 of the Digital Administration Code (CAD, Legislative Decree 82/2005).

15 The definitions of these categories are contained in Articles 4 and 9 of the European General Data Protection Regulation (EU) 2016/679 and Article 3 of the European Regulation on the Free Flow of Non-Personal Data (EU) 2018/1807.

The progressive development of *smart cities* has also contributed to an exponential increase in the amount of non-personal data stored by the PA. This scenario has recently moved forward with the 2019-2021 Three-Year Plan for IT[16], drawn up by the Agency for Digital Italy (AgID).

The introduction of the *Smart Landscape*[17] concept marks an important change in the long-held notion of *smartness* in the collective imagination, which referred to a wide range of services and benefits for citizens, relegating businesses and industry to the margins of the projects devised from time to time. On the other hand, the Smart Landscape model envisages the development of services for businesses, especially those related to goods logistics.

It is worth mentioning that the Three-Year Plan foresees the progressive implementation of a predictive model (Smart Landscape Engine) to be used in the governance of the Smart Landscape. The SLE will be able to develop *what-if* scenarios based on the information entered and will support decision-making processes for the development of the *smart landscape*. This is clearly a significant development: the creation of an artificial intelligence model for the PA marks a further move[18] by

16 Available at the following link https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/index.html.

17 The limitations of the Smart city paradigm necessarily led to the evolution of the Smart landscape model. The 2019-2021 Three-Year Plan describes those shortcomings as follows:
"*The initiatives carried out so far on this subject, particularly by some metropolitan cities, are commendable but suffer from a narrow approach that considers only the reference urban context. Also, most of them focus on aspects related to the 'citizen' and ignore factors that have a strong impact on businesses, such as, for example, the movement of goods and the opportunities arising from integration with other subsystems (Port Communities, Cargo communities, territorial logistical nodes, distribution companies, etc.).*
[...] Logistics is a strategic sector for the national economy and should be considered as a tool of industrial policy, to continuously enhance the production system and to promote the development of eco-sustainable transport and environmental protection.
The 'Internet of Things' paradigm applied to goods implies the integration of services provided by different public/private actors that can be achieved through the complete digitalisation of the logistics chain.
Smart solutions based on the use of interconnected logistical corridors and nodes make it possible to overcome the sector's complexity – compounded by the multimodal nature of transport and the number of players involved – and to recover considerable areas of efficiency, thereby optimising the time and cost of moving goods and guaranteeing safety and security.
Therefore, careful attention should be given to this wide-ranging, complex system, including a multiplicity of 'logistic nodes' (ports, airports, freight villages, interports, territorial logistics platforms, distribution centres, and companies, etc.) and the intermodal links between them. The latter is necessary to make the logistics environment – including all the logistics nodes and the cities – function as a whole, adopting a synergic, coordinated and integrated approach aimed at the optimisation of investments and efficiency and the development of a system of synergies and the implementation of 'sustainable logistics' (economic, environmental, social sustainability).
[...] The national programmes that have been and are being implemented should therefore be synergised in a broader perspective in order to make the already developed vertical solutions interoperable in order to achieve intelligent and safe management of mobility, people, and goods, and to promote the development of services based on the needs of citizens and businesses".
Therefore, there is a clear push towards an integrated model of personal services and business services/logistics.

18 Article 50 of the CAD already allows the PAs, as part of their institutional functions, to analyse data, also in combination with that held by other PAs, by public service managers, and by publicly controlled companies, except for listed companies that do not manage public services.

the public sector towards technologies (and practices) already widely used in the private sector.

Administrative transparency and *open data* are not the focus of this paper. Suffice to say here that public sector data governance cannot, in practice, disregard publication obligations or the guarantee of full accessibility and re-use of information (SCIACCHITANO, 2018, p. 281). This information, having been duly evaluated and balanced vis-a-vis the right to protection of the personal data of data subjects, contributes significantly to increasing the set of data that can both be correlated with other data and be a factor of global disclosure (CALZOLAIO, 2016, p. 601) of personal and non-personal information.

Digitisation, the development of ICT, and the progress of Artificial Intelligence have exceptional potential for improving the quality of public sector services and can significantly contribute to simplification, cost reduction, transparency of administrative action, the exercise of citizenship rights, and the proper conduct of democratic life. Recent global events have demonstrated their usefulness also in the management of complex situations such as epidemic containment (the facility of having organised data and the interoperability of databases belonging to different public and private bodies seem, in some cases, to have made a difference[19]).

However, having an enormous amount of information centralised in a database, together with the ability to cross-reference this information with that of other databases using highly sophisticated algorithms, brings with it serious risks for the rights and freedoms of individuals, especially concerning possible discrimination and for the stability of democratic systems, should the information be used to interfere with the free formation of public opinion[20] or with the conduct of the political, economic and administrative activities of a sovereign State[21].

In this regard, it should be noted that, after conducting a joint cognitive analysis of the Big Data issue[22], the Data Protection Authority, the Italian Communications

19 The Veneto Region's pandemic management model, although raising complex legal issues that we shall not go into here, appears to be an example of the effective use of databases to combat the health emergency.

20 An example, which considers the use of Deep Fake techniques, see BERTONI F., *Deepfake, ovvero Manipula et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, in Ciberspazio e diritto, v. 20 nº. 62 (1-2-2019), pp. 11-28.

21 For the potential and risks of using Big Data in the public sector see RUOTOLO G.M., *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in Studi sull'integrazione europea, XIII (2018) pp.105 ff; more generally, on opportunities and risks of democracy in the "digital era", COSTANZO P., *La democrazia digitale (precautions for use)*, in Diritto pubblico, I, January-April 2019.

22 Autorità garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la protezione dei dati personali, Indagine conoscitiva sui Big Data, final document, 10 February 2020, available at

2022 | v. 16 | n. 1 | p. 1-32 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v16n115229

Regulatory Authority (AGCOM), and the Italian Competition Regulatory Authority (AGCM) expressed concern about certain Big Data analysis activities' compatibility with data protection legislation. The problem areas included the vagueness of the analysis purposes, the risks related to the possibility of re-identifying of the data subjects, and the opacity of the logic applied by the algorithms.

The report explicitly references the creation of the National Digital Data Platform, introduced by Article 50-ter of the Digital Administration Code (CAD). The critical issues of the platform should be largely to do with the centralisation of "*sensitive and highly sensitive*" information in a single entity, for entirely generic purposes, with an obvious risk of misuse. Given these premises, the three Independent Authorities believe that Big Data-based processing in the public sector will require a suitable legal basis

> [...] that assures citizens not only of the transparency of the decisions but also of the proportionality of the legal recourse to such methodology as regards the public interest objective pursued and the identification, in respect of the principle of privacy by design, of adequate guarantees to be built into the processing, after having carefully evaluated the acute risks for the rights and liberties of data subjects[23].

3. The babel of data: end of classifications?

The expansion of Big Data Analytics seems to have highlighted the limitations of the cumbersome process of categorising data. Although this activity is feasible in ex-ante reconnaissance of datasets, it is often of little use ex-post, i.e., following the data processing with machine-learning tools. As is well known, very refined algorithms now allow us to extract personal information on an individual even from information that is not personal[24].

The use of algorithms applied to a huge volume of data makes it possible to extract or even predict personal information, sometimes from non-personal informa-

this link https://www.agcom.it/documents/10179/17633816/Documento+generico+10-02-2020+1581346981452/39c08bbe-1c02-43dc-bb8e-6d1cc9ec0fcf?version=1.0.

23 Ibid, pp. 68-69.

24 For all, D'ACQUISTO G., NALDI M., *Big data e privacy by design*, Giappichelli, Turin, 2017, in particular Chapter 1, *Big Data e protezione dei dati personali*.

tion, correlated with other datasets of different origin and content[25]. In this context, the distinction between personal and non-personal data becomes less and less achievable[26], and the possibility of applying different legal regimes to different types of data becomes less and less likely.

If such a distinction were possible, it would entail an increase in expenditure for technological adaptations and the adoption of internal regulatory commitments by public administrations, which do not appear feasible in the short term. Also, in the private sector, such a burden would lead to a significant increase in costs and a reduction in the value of the data itself.

The problem now arises following the entry into force of the European Free Flow of Data (FFD) Regulation concerning the circulation of non-personal data. The rule introduces a differentiated regime for all data that does not fall within the definition[27] (and governance) contained in the GDPR. As is well known, the possible difficulty in separating the two sets of data has already been provided for by European legislation, which, in Article 2, para. 2 of Regulation 1807/2018, specifies that were personal and non-personal data within a dataset are inextricably linked, the application of the GDPR remains unaffected. In the author's view, this legal framework will constitute a significant obstacle to the free circulation of a very large amount of non-personal data, which is nevertheless inextricably linked to personal data[28].

Continuing the review of data types, with specific reference to processing carried out by public administrations, there is a further classification criterion that, in practice, proves to be very impactful. It hinges on the distinction between datasets contained in paper documents and datasets that constitute the digital documents of the PA. This distinction is not merely formal but concerns substantial aspects, as we shall see.

Once again, the FFD Regulation divides, stating that "*processing*" is defined as "*any operation or set of operations performed upon data or sets of data in electronic form*[29]".

25 Autorità per le Garanzie nelle Comunicazioni, *Big Data. Interim report within the framework of the fact-finding investigation referred to in Resolution No 217/17/CONS*, available at https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0 p. 14.

26 See Ibid, Executive Summary, p. 7.

27 Article 3 No. 1 of Reg. 2018/1807 defines *data* as "*data other than personal data as defined in Article 4(1) of Regulation (EU) 2016/679*".

28 Article 8 of the same article confirms the concerns. It provides for the Commission to prepare, by 29 November 2022, a report on the implementation of the Regulation, focusing specifically on mixed sets of personal and non-personal data in relation to unforeseeable future technological developments.

29 Reg. No. 2018/1807, Article 3 no. 2.

2022 | v. 16 | n. 1 | p. 1-32 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v16n115229

As mentioned above, the FFD Regulation lays down rules to facilitate the free movement of data, which are only applicable to the data processing in electronic format.

Non-personal data contained in paper documents are de facto excluded from the rules governing their free movement within European Union territory. Failure to take account of the existence of this "double track" is likely to give a partial view of reality; such a peculiarity could lead to significant limitations in the application of the legislation and ultimately reduce its effectiveness.

4. Rules and roles for data storage in the PA

The general regulatory references on the storage of Public Administration documents and the archives management are contained in Presidential Decree 445/2000, particularly Article 68[30]. This same provision makes it compulsory to apply privacy legislation to all document management and storage activities. Therefore, it will be useful here to quickly recall the *data storage* rules laid down by the GDPR.

EU Regulation 2016/679 requires the data controller[31] to store personal data for a period of time not exceeding the purposes for which they were processed, with only two exceptions: where the individuals to whom the personal data relate are no longer identifiable; where the data are processed for archival purposes in the public interest, for scientific or historical research or for statistical purposes (Article 5 para. 1(e)).

The GDPR also requires the data controller to inform the data subject of the storage period for personal data or at least to indicate the criteria used to determine that period Article 13 para. 2(a). As will be seen shortly, the data processor[32] must also delete or return personal data to the controller once the service has been completed (Article 28, para. 3(g)). The Register of processing operations should indicate, where possible, the latest deletion dates for each category of personal data (Article 30 para. 1(f)).

In the author's view, there are two aspects of the privacy rules on storage that significantly affect, more than others, the governance of public sector data.

30 The storage and discarding ceilings rules and the scrutiny of the Archival Superintendency further define the management framework for public archives.

31 The data controller is the natural or legal person, public authority, service, or other body that determines the purposes and means of the processing of personal data (GDPR, Article 4, no. 7).

32 This means the natural or legal person, public authority, service, or other body that processes data on behalf of the data controller (Article 4(8)).

The first of these is the application of Article 25 of Regulation 2016/679. The rule requires the data controller to implement technical and organisational measures to ensure data protection and thereby protect the rights of data subjects. These measures will have to be identified after a case-by-case assessment for each different case of processing, "*taking into account the state of the art and the cost of implementation, as well as the nature, scope, context and purposes of the processing, and the risks to the rights and freedoms of natural persons which are of varying likelihood and severity [...]*".

The direct consequence of the application of the principle of privacy by design just described in what we have termed a "double-track" in the previous paragraph is obvious: the storage of administrative documents will be subject aborigine to two different rules, depending on whether the documents are paper or digital[33].

The existence of a dual data storage system is also a factor that cannot be eliminated in the short term. This is confirmed by the CAD rule, which provides for PAs to draw up plans to replace paper-based archives with computer-based ones following a cost-benefit assessment[34].

A second and even more relevant aspect of the application of the privacy rules to public sector data storage concerns the identification and appointment of the aforementioned external data processors, pursuant to Article 28 of the GDPR.

The GDPR lays down rather precise rules for the attribution of responsibility with regard to the lawful processing of data. The data controller is responsible for deciding on the purposes and means of processing. On the other hand, data processors are persons who process the data on behalf of the data controller and are to this end "appointed" by contract or an alternative legally binding act. This act contains the rules for the relationship between the data controller and the person appointed[35], the instructions are given by the former, and the latter's obligations regarding the processing of personal data.

In the public administration context, many activities are managed by external parties appointed following a call for tenders or through direct awarding. This means that substantial amounts of data are processed externally in many areas.

33 By the way only of example, the outcome of the discarding activity in the paper archive will involve the physical destruction of the documents by sending them to be shredded – an activity to be entrusted to specialised companies; the same activity will obviously be carried out in a different way in digital archives.

34 Legislative Decree 82/2005 (Article 42).

35 "[...] *the subject matter covered and the duration of the processing, the nature, and purposes of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller*" (GDPR, Article 28 para. 3).

It is not even possible here to mention the complex organisation chart of 'privacy roles' resulting from the network of relations linking the PA to other public bodies and private sector companies and professionals. However, it should be noted that compliance with data protection regulations also imposed certain requirements during the Covid-19 pandemic. Indeed, compliance with the GDPR and the Privacy Code required state authorities to quickly draw up regulations that allowed the numerous actors involved in managing the emergency to process personal data legitimately. Although undoubtedly necessary and urgent, this activity has given rise to a complex network of roles and responsibilities that are honestly difficult to reconstruct in retrospect[36].

After this digression, it is now necessary to identify the entities in charge of data storage in the Public Administration; if such parties are external to the administration itself, they will have to be contracted under Article 28 of the GDPR.

Article 34 of the CAD offers public administrations the alternative between storing computerised documents within their organisational structure and entrusting this activity to public and private entities accredited by AgID as conservators. Article 44 requires that the storage manager who decides to outsource must identify entities offering "*appropriate organisational, technological and personal data protection guarantees*". Compliance with this last requirement must be ensured through the drafting and signing of contracts pursuant to Article 28, which contains the legal regulation of the relationship between the data *controller* and *data processor*, as well as stringent instructions on the computer security of processed data. The centrality and relevance of this "privacy fulfilment" have recently been confirmed by the Data Protection Authority.

In its 13 February 2020[37], opinion on the draft Guidelines on the formation, management, and storage of computerised documents[38], the Data Protection Authority reiterated the need for PAs to meet the requirements of the GDPR, stating that a

36 The reference is to Article 17 bis of the so-called Cura Italia/Heal Italy law (Decree-Law 17 March 2020, No. 18 converted with law No. 27 of 24 April 2020), which lists a long series of entities who, in order to be able to manage and contain the Covid-19 health emergency, are authorised to process data related to articles 9 and 10 of the GDPR and to use them in communications.

37 Data Protection Authority, *Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"* – 13 February 2020 available at the link https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9283921.

38 The draft is available at https://docs.italia.it/AgID/documenti-in-consultazione/lg-documenti-informatici-docs/it/bozza/index.html.

clear allocation of tasks is a prerequisite for the proper allocation of responsibilities, and this division must be contractualised and set out in clauses that meet the requirements of the European Regulation, especially so in cases where services are to be outsourced.

It is worth emphasising that the Authority does not set any limits to the private outsourcing of services involving the processing of personal data but insists, instead, on the full application of all the guarantees identified by the GDPR (contractualisation of external data controllers, compliance with security obligations, application of the principles of privacy by design and by default, efficient notification procedures in the event of data breaches and adherence to codes of conduct).

Having recalled the rules and roles of public data storage, we will now turn to the system for the physical location of stored data and documents. In the following paragraphs, at least two important aspects will be considered: identifying the type of storage infrastructure and the rules of data localisation.

5. The identification of infrastructures: from paper archives to the cloud first principle

Public administration data are now only stored in digital format, in accordance with the *digital-first* principle.

Article 40 of the Digital Administration Code requires that public administrations create the originals of their documents by electronic means, and Article 43 clarifies that the obligations to preserve documents are deemed to be fulfilled for all legal purposes by electronic documents if they conform to the originals and the guidelines.

As mentioned in the previous pages, the CAD provides for the preparation of plans for the gradual replacement of paper-based archives with computer-based ones. As a result, paper archives are now subject to what could be described as a "while stocks last" system. But on closer inspection, the above mentioned Article 42 of the CAD links such determinations to a cost-benefit assessment and does not indicate a maximum deadline for completing the transition from paper to digital archives. This aspect, left to the discretion of each individual administration and combined with the lack of a deadline for completing the switch-over, seems to be slowing down the PA digitalisation process.

2022 | v. 16 | n. 1 | p. 1-32 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v16n115229

Having said that, let us now look at some significant State interventions in implementing the Digital Agenda[39], which have affected data governance.

One of the cross-cutting actions of the country's Digital Growth Strategy envisages the gradual adoption of the *cloud computing*[40] paradigm. The 2019-2021 Three-Year IT Plan (PTI), implementing this policy choice, contains a strong option for cloud services and infrastructure. This option was enshrined in the "*cloud-first*" principle[41].

The PTI outlines a path for transforming PA information systems with the aim of moving from the current fragmentation and lack of homogeneity to an evolved and efficient organisation.

This transformation should be based on three key elements: the application of the aforementioned *cloud-first* principle when defining new projects and programming new PA services; the gradual migration of existing infrastructures and services to the cloud (known as *cloud enablement*); and finally, the strengthening of skills through the creation of dedicated centres, to consolidate know-how and experience related to the management of cloud services in PA.

According to the PTI, these Competence Centres should be forums composed of technicians, experts, and IT managers "*who discuss and propose standards and regulations for digital services, and who share information, solutions and skills to help maintain, update and increase the reliability of systems*"[42].

The strategy for adopting cloud computing is also being executed through constraints on ICT spending. PAs implementing the 2019-2021 Three-Year Plan can no longer invest in hardware and infrastructure. However, expenditure and investment are possible for virtualisation projects and the migration of services to the PA Cloud infrastructure.

39 "The *aim of the Digital Agenda is to leverage the potential of ICT technologies to foster innovation, progress and economic growth, with the development of the digital single market as its main objective.*
In the framework of the European Digital Agenda, Italy has developed the Italian Digital Agenda, a national strategy to achieve the objectives set out in the European Agenda", see http://www.funzionepubblica.gov.it/digitalizzazione/agenda-digitale.

40 See https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf , p. 61.

41 "*In accordance with the Cloud First principle, PAs must, when defining a new project, and/or developing new services, adopt the cloud paradigm, in particular SaaS services, before any other technological option*", see https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/cloud-enablement.html.

42 Ibid.

No less important is the fact that the option of cloud computing certainly meets the need to reduce the costs of IT infrastructures[43], in line with the criteria of efficiency, effectiveness, and cost-effectiveness also referred to in Article 12 of the CAD[44].

This choice seems to be the core of a wider strategy to rationalise the information assets of the Public Administration[45]. It, therefore, marks a cultural, rather than technical or legal, transformation of no small importance if read in the light of the oft-mentioned trend of global digitisation.

On this front, and before moving on to the second question concerning the location of the data, it is of some relevance to mention the *Digital Economy and Society Index (DESI)*, the findings of which were published on 11 June 2020[46]. The European Commission uses this index to monitor the digital progress of the EU Member States.

The overall ranking shows the sum of the data collected with reference to five thematic areas: connectivity, human capital, use of internet services, integration of digital technologies, and digital public services. Italy's positioning in 25th place out of 28 speaks loud and clear, and prompts more than one reflection[47].

Alongside satisfactory results, for example, for connectivity (in particular "5G readiness", where Italy is well above the European average), the DESI highlights very serious shortcomings with respect to human capital, an area in which Italy ranks last in Europe. Only 42% of 16-74 year-olds have basic digital skills (compared to the EU average of 58%), and only 22% have more than basic digital skills (compared to 33% in the EU). The modest use of the internet and the type of content searched online by users[48] would directly consequence the low digital skills found through the European survey.

43 Cfr. https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/perche-usare-il-cloud.html#riduzione--dei-costi: "*Cloud applications (SaaS) are generally paid for on a per-use basis; they allow you to manage the growth of a service dynamically and require very little initial investment. [...] The low initial investment means a reduction, so it is possible to develop and test solutions on a small scale, which can be quickly evaluated and then adopted, radically changed or abandoned, at minimal cost*".

44 "*In organising their activities autonomously, public administrations shall use information and communication technologies to achieve the objectives of efficiency, effectiveness, economy, impartiality, transparency, simplification and participation* [...]". See in this regard MASUCCI A., *Digitalizzazione dell'amministrazione e servizi pubblici online. Lineamenti del disegno normativo*, in Diritto Pubblico, I, January-April 2019, pp. 140 ff.

45 Significant rationalisation based on central IT coordination. According to Article 14 of the CAD, "*AgID ensures the IT coordination of the state, regional and local administration [...]*". On this point DI FRANCESCO TORREGROSSA M., *La competenza statale nel processo di digitalizzazione delle pubbliche amministrazioni*, in Consulta online, 2019 Folder I, pp. 64 ff.

46 The digital performance of all EU countries can be examined at this link https://ec.europa.eu/digital-single-market/en/countries-performance-digitisation.

47 The Italian scoreboard can be viewed at this link https://ec.europa.eu/digital-single-market/en/scoreboard/italy.

48 79% of users use the Internet to enjoy music, videos, and games.

Nevertheless, the European Index acknowledges the Italian State's growing commitment to efficient digitalisation, a commitment demonstrated, among other things, through the establishment of the Ministry for Technological Innovation and Digitalisation, the presentation of the "Italy 2025" strategy and the preparation of a three-year plan for IT in PA containing an "*exhaustive list of objectives for the coming years*".

This commitment is evidenced by the excellent results achieved in online public services, digital public services for businesses, and open data, areas where Italy even exceeds the European average. However, this figure, far from being reassuring, is actually mortifying: despite the results just mentioned, Italy is in 19th place in the digital public services league table. The element that invalidates the overall result is the "*low level of online interaction between public authorities and the general public. Only 32% of Italian online users actively use e-government services (compared to the EU average of 67%)*[49]".

It should be noted that such a serious lag can only have very serious repercussions for the country's participation in the Digital Single Market. However, awareness of these serious shortcomings, and above all, of the imbalance between the development of PA digital innovation programmes and the scant attention paid to the "digital" rights of citizens and businesses, as guaranteed by the CAD[50], could be an opportunity to make an organic and structured investment in digital literacy[51]. Therefore, if not tackled quickly, the digital divide risks proving to be by far the most difficult obstacle to remove for Italy's participation in the Digital Single Market[52].

Moreover, the direct connection between data literacy, participation in the digital economy, and technological sovereignty is a presupposition of the European digital strategy, recently confirmed in the White Paper on artificial intelligence[53].

49 Scoreboard Italy, See Supra note 52, p. 14.

50 Article 3 recognises the right of everyone to access and effectively use the solutions and tools provided by the CAD in their relations with public administrations.

51 As required by Article 8 of the CAD.

52 On the key-role of digital literacy for the development of the Digital Single Market See PAGNANELLI V., Accesso, accessibilità... cit., p. 212: "*The rapid and irreversible evolution towards digital administration makes it an absolute priority to overcome the digital divide and to consequently take steps in that direction. These measures must include a serious investment in digital literacy*".

53 European Commission, COM (2020) 65 final, 19/02/2020, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, p. 4, "*Harnessing the EU's capacity to invest in next generation technologies and infrastructures, as well as in digital competences, such as data literacy, will increase Europe's technological sovereignty in key enabling technologies and infrastructures for the data economy*".

6. Location rules: public data storage and sovereignty

The second important aspect regarding the location of public sector data relates to the physical location of the storage infrastructure, as the law sometimes requires that certain datasets are stored in servers located on national territory.

Again, a few examples will help clarify the question's terms.

The most recent case of imposing a location obligation in Italy can be found in Article 6 of Decree-Law No. 28 of 2020. This is the "*Covid-19 alert system*" regulation, which introduced a platform for the management of the infection tracking system and required this platform to be located on national territory[54].

As mentioned in the introduction, the Personal Data Protection Authority made an explicit recommendation to this effect during the consultation phase, recalling the precautionary principle as regards the type of data being processed and thus the high risks for citizens using the contact tracing[55] app.

At the end of an investigation and information-gathering exercise launched because of possible risks to national security, the Parliamentary Committee for the Security of the Republic (COPASIR) also sent Parliament a report on the Covid-19 alert system[56]. The Committee, after referring to the need for data storage to take place on the national territory, expressed concern about the composition of the company that owns the app chosen (Immuni). In fact, a minority share of Bending Spoons S.p.A. is said to belong to a fund owned by a Chinese businessman. The concerns expressed by COPASIR stem from China's Cybersecurity Law, which "*generally obliges citizens and organisations to provide support and assistance to military public security authorities and intelligence agencies*[57]".

The report's conclusions become even more explicit when they expressly refer to non-negligible and unmitigated geopolitical risks. These risks would be mainly related to the necessary and non-fungible presence of *non-domestic private partners* in

54 According to Article 6, the single national platform for the management of the alert system "*is publicly owned and is implemented [...] exclusively with infrastructures located on national territory*".

55 See supra note 7.

56 Parliamentary Committee for the Security of the Republic (COPASIR), *Report on the security profiles of the Covid-19 alert system provided for in Article 6 of Decree-Law No 28 of 30 April 2020*, 13/05/2020, available at http://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/002/INTERO.pdf.

57 Ibid, p. 11.

the implementation of the contact tracing IT system; these entities, COPASIR warns, could manipulate the data for purposes other than those for which they were collected, namely, of a "*political, military, health or commercial*[58] nature".

Another location requirement is stated in the aforementioned Guidelines on forming, managing, and storing electronic documents released by AgID in draft for consultation. In the section on infrastructures, there is a requirement that the storage systems of public administrations and accredited conservators provide for "*the material storage of data and back-up copies on national territory*" in order to allow the Agency for Digital Italy to perform its supervisory functions[59].

It is useful to recall that, based on the opinion of the Council of State, once the Guidelines have been adopted by AgID pursuant to the procedure indicated in Article 71 of the CAD, they will acquire a binding character, will have erga omnes validity and will be actionable before the administrative courts[60].

A peculiarity of the Italian system's data location rules should be highlighted at this point. In fact, in the Cloud section of the Three-Year Plan for IT in the PA, specifically in the list of frequently asked questions, it is stated that PAs may choose service providers such as Google Cloud, Azure or others, provided they are qualified in accordance with AgID circular No. 3 of 9 April 2018, for the use of IaaS and PaaS services[61].

Infrastructure as a Service cloud services can provide *computing*, *networking*, and data *storage* services. The fact that AgID's Cloud Marketplace[62] includes IaaS service providers that do not offer users the option of choosing the location of the sites where data will be stored and processed, which contravenes the location obligations mentioned above, seems to reveal a gap in the coordination of the many aspects of the complex governance of public data.

In addition to the aforementioned legal and regulatory provisions, the Personal Data Protection Authority has yet again pronounced the location of personal data, at the instigation of the Union of Criminal Chambers in recent months. The reference is to the letter sent by the President of the Authority to Minister of Justice Alfonso

58 Ibid, p. 13.
59 Guidelines on forming, managing, and storing electronic documents, draft, see Supra note 43.
60 Ibid, Chapter 1.10.
61 See https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/domande-frequenti.html#circolare-qualificazione-cloud-service-provider.
62 See https://cloud. italia.it/marketplace/show/all?searchCategory=IaaS.

Bonafede concerning the software used to allow criminal proceedings to be conducted remotely[63]. The subject of the clarification request was the choice of platforms for the conduct of criminal hearings, provided by a technology partner (Microsoft) based in the United States, and therefore subject to the application of the Cloud Act, which "*gives the US authorities broad power to acquire data and information*".

The location obligations imposed on Italian public administrations, combined with references to Chinese and US legislation, take us to the heart of the matter.

Vincenzo Zeno-Zencovich effectively summed it up when he commented on the Schrems Case[64], "*establishing how personal data collected through telecommunications networks should and/or can be processed and under what conditions they can be transferred to other countries is simply the expression of the exercise of sovereign powers by and according to the rule of law*[65]".

A few brief references to China's cybersecurity legislation and US cloud computing legislation allows us to highlight the precise strategic choices made to defend state sovereignty within (and beyond) the territorial limits of its jurisdiction.

Bearing in mind that China's highly structured normative and regulatory system in matters of privacy and cyber security[66] is neither easily accessible nor decipherable for foreign scholars, we shall refer in the following paragraphs only to some particular traits of Chinese data governance.

---

63 Personal Data Protection Authority, *Remote criminal trial: letter by the President of the Personal Data Protection Authority, Antonello Soro, to the Minister of Justice, Alfonso Bonafede*, 16 April 2020, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316889.

64 The well-known judgment by which the EU Court of Justice declared the invalidity of EU Commission Decision No 2000/252/EC on the so-called Safe Harbour agreement regarding the transfer of personal data of European citizens to the US. On the Schrems case, see, ex plurimis RESTA G., *La sorveglianza elettronica di massa e il conflitto regulativo USA/UE*, in La protezione transnazionale dei dati personali. From "Safe Harbour principles al "Privacy Shield", edited by G. Resta, V. Zeno Zencovich, Consumatori e Mercato series, Roma Tre press, Rome, 2016, pp. 23-48; BONINI M., *Sicurezza e tecnologia, fra libertà negativa e principi liberali. Apple, Schrems and Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in Rivista AIC, 3/2016 FIORILLO V., *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in Federalismi.it, 26 July 2017. A new chapter in the story has recently appeared with the 16 July 2020 publication of the judgment in Case C-311/18 Data Protection Commissioner v Maximilian Schrems and Facebook Ireland, whereby the Court of Justice of the EU declared Commission Decision 2016/1250 invalid concerning the adequacy of the protection offered by the so-called Privacy Shield EU-US for the transfer of personal data to the United States.

65 ZENO ZENCOVICH V., *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in La protezione transnazionale dei dati personali. From "Safe Harbour principles al 'Privacy Shield'", cit. p. 11.

66 For contextualisation see GREENLEAF G., *Asian data privacy law. Trade and Human rights perspectives*, Oxford University Press Oxford, 2014, pp. 192 ff.; LINDSAY J.R., CHEUNG T.M., REVERON D.S., *China and cybersecurity espionage, strategy, and politics in the digital domain*, Oxford University Press, Oxford, 2015, in particular, Ch. 10; AUSTIN G., *Cybersecurity in China. The next wave*, Springer, 2018.

2022 | v. 16 | n. 1 | p. 1-32 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v16n115229

The *Cybersecurity law*[67], passed in November 2016, lays down a series of principles since then supplemented by a large number of laws, regulations, and standards that provide technical guidance for the implementation of the national *cybersecurity*[68] system. It is important to highlight that this law does not focus on the protection of personal data (although it contains rules to that effect) but rather on the protection of State sovereignty, which is considered to be the highest priority[69]. The first article lists the safeguarding of *cybersecurity* and *cyberspace sovereignty* as one of its aims, followed by protecting the rights of citizens and businesses and the increased computerisation of the economy and society.

Network operators, who are the main recipients of the rules laid down in the *cybersecurity law*, must adapt their infrastructures to a series of technical requirements aimed at ensuring cyber security. The obligations will be more or less stringent depending on the type of infrastructure managed[70]. Network operators are also explicitly required to cooperate with the public security authorities in order to safeguard national security (Article 28).

An interesting contribution by Aimin, Guosong, and Wentong[71] breaks down the principle of Chinese cyber-sovereignty into four fundamental rights: the right to jurisdiction, i.e., the right to manage the computer networks that exist on the national territory; the right to defend against computer attacks and threats outside from the country; the right to independence, i.e., the right to use the services of ICTs using exclusively national networks, independent of the power of other States (the reference here is to the US DNS); and lastly, the right of equality, which gives each State the right of jurisdiction over its computer networks[72].

67 For an analysis of the content of the cybersecurity law, see HUANG L., ILAN D., MOONEY CARROL K., ZHOU Z., *Understanding the impact of China's far-reaching new cybersecurity law*, in Intellectual Property & Technology Law Journal, v. 30 nº. 2, February 2018, pp. 15 ff.; AIMIN Q., GUOSONG S., WENTONG Z., *Assessing China's cybersecurity law*, in Computer Law & Security Review 34 (2018), pp. 1342 ff.

68 National standards and technical guidances are further subdivided by type into mandatory standards (GB Standards), voluntary standards (GB/T Standards) and technical guidance (GB/Z guidance).

69 See AIMIN Q., GUOSONG S., WENTONG Z., cit., p. 1344. Italy has adopted its cybersecurity law with Decree-Law Nº. 105 of 21 September 2019, converted with Law No 133 of 18 November 2019, which established the national cyber security perimeter.

70 Chinese law provides for an "aggravated" regulation for operators of Critical Information Infrastructure, defined as "*infrastructure that is used in public communications and information services, energy, transportation, water conservancy, finance, public services or electronic governance or that, if it were destroyed, malfunctioned or leaked data, could seriously endanger national security, national welfare, and the people's livelihood, or the public interest*", see HUANG L., ILAN D., MOONEY CARROL K., ZHOU Z., cit. pp. 17 ff.

71 AIMIN Q., GUOSONG S., WENTONG Z., *Assessing China's Cybersecurity Law*, cit.

72 Ibid, pp. 1345-1346.

It is no coincidence that one of the regulatory tools that *cybersecurity law* identifies to assert its cyber sovereignty is the imposition, on *Critical Information Infrastructure*[73] operators, of the obligation to locate personal data and the important data generated and collected by them, exclusively on national territory[74].

Let us now turn to the United States, where the government, after launching its *Cloud First Strategy* in 2011, is now preparing to evolve from the *Cloud-First* paradigm to *Cloud Smart*, based on three pillars: *security*, *procurement*, and *workforce*[75]. More relevant to the purposes of this paper is certainly the regulation introduced with the *Cloud Act* concerning the US Authorities' access to data stored outside the territory (and jurisdiction) of the USA.

In fact, the Clarifying Lawful Overseas Use of Data (CLOUD) Act[76], passed at the beginning of 2018, allows US authorities to access information contained on the servers of US companies anywhere in the world, in order to facilitate the investigation and prosecution of crimes. At the same time, it allows foreign governments to access data stored on US territory for the same purposes. The mechanism is based on a system of *executive agreements* negotiated bilaterally with individual governments[77] — an arrangement that in fact overlaps with the Mutual Legal Assistance Treaties model, which is considered inefficient because it is too slow and cumbersome[78].

The declared aim of the US government is to avoid conflicts of jurisdiction with other sovereign States, while ensuring procedural safeguards for all cases of access to personal data.

---

73 See Supra note 76.

74 "*Specifically, the data required to be stored locally in accordance with other laws or regulations include: population and health data (Section 10 of the Provisional Measures on Population Health Information Management), credit information (Section 24 of the Rules on Credit Industry Administration), personal financial information (Article 6 of the People's Bank of China Notice on the Protection of Personal Financial Information), map data (Section 34 of the Rules on Map Management), online publication data (Article 8 of the Regulations on the Administration of Online Publishing Services); data related to online car-hailing business (Article 27 of the Provisional Measures on Online Car-hailing Operation Service Management)*", AIMIN Q., GUOSONG S., WENTONG Z., *Assessing China's cybersecurity law*, cited above, p. 1351.

75 See https://cloud.cio.gov/strategy/.

76 The text of the Cloud Act can be found at https://www.justice.gov/dag/page/file/1152896/download; the US Department of Justice published the white paper in April 2019 and is available at https://www.justice.gov/opa/press-release/file/1153446/download describes its background, features, and purpose.

77 See Cloud Act, Supra, *Sect. 105. Executive agreements on access to data by foreign governments* list the requirements that the foreign government must meet in order to enter into a bilateral agreement.

78 "*Mutual Legal Assistance Treaties is a long-established way for the US government to access private information held abroad. These agreements permit a public authority seeking data to ask for the country's assistance in which the data is held and require that country to cooperate in processing such requests under its domestic law. MLATs establish legal mechanisms for cooperation between signatory nations in criminal matters and proceedings, including exchanging evidence and information during criminal proceedings*", SCHWARTS P.M., Legal access to the global cloud, in Columbia Law Review, v. 118:1681, 2018, p. 1720.

The outcome, as we know, is very controversial. Some commentators have raised doubts about the risks brought by a significant reduction of privacy protection compared to the previous MLATs mechanism. Others, however, argue that this system is fully aligned with that posed by the GDPR. Indeed, Article 48 of the European Regulation, which regulates unauthorised transfers of data outside the European Union in cases where they are based on a judgment or administrative decision of a third State, outlines a hypothesis for recognition of such acts precisely where there is an international agreement, such as a mutual legal assistance treaty[79].

In this respect, it is interesting to note that the European Union is moving in the same direction as the United States in adopting a Regulation on access to electronic evidence; its imminent proposal is being discussed in the Council[80], and it will have an approach that largely overlaps with the Cloud Act model.

From the brief analysis of the recently proposed Chinese and US "digital strategies", it seems possible to draw confirmation of the inseparable link between data governance and the assertion of (digital) State sovereignty.

We need merely recall that the Chinese and US policy choices mentioned above have resulted firstly in other States adopting defensive measures for their own information assets; secondly, large service providers have had to adapt to the rules imposed in order to avoid being excluded from very large shares of the global market.

It is no coincidence that the Big players quickly have, on the one hand, set up data centers on the territory of the People's Republic of China and, on the other, have developed solutions that, while complying with the law, effectively allow their customers to escape possible unwanted access to their information by the US Government under the Cloud Act[81].

79 On the critical aspects of the mechanism introduced by the *Cloud Act*, see ABRAHA H.H., *How compatible is the US "Cloud Act" with cloud computing? A brief analysis*, in International Data Privacy Law, 2019, Vol. 9 no. 3, pp. 207 ff.; against BRENNAN M.W., MAXWELL W., SURA A.A., *Demystifying the Cloud Act: assessing the law's compatibility with international norms and the GDPR*, Hogan Lovells, January 2019, who argue that the safeguards introduced by the *Cloud Act* are up to international data protection standards, including the GDPR.

80 *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD)*, available at this link https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN.

81 The *Data Trustee model* developed by Microsoft for the German market is an example of such solution. See https://docs.microsoft.com/en-us/azure/germany/germany-overview-data-trustee; on this subject, see. ABRAHA, H. H. *How compatible is the US "Cloud Act" with cloud computing? A brief analysis*, cit., p. 208: "*This arrangement [the Data trustee model, N.d.A.] could create a situation where personal data concerning a US person and required for US domestic crime investigation purpose is neither located in the USA nor effectively controlled by a US company*". The *data trustee* model developed by Microsoft allows the company to retain responsibility for the service from a technical point of view while at the same time respecting the need to localise the data in Germany so that it is exclusively subject to

7. Concluding remarks: the european digital strategy

The European strategy is on a different level from all of the above.

In fact, the document "*A European Strategy for Data*[82]", published on 19 February 2020, sets out a vision of the European Union in the global context; the plan has a very precise identity and is significantly different from those of other global players.

The document, based on an analysis of the roles of the US and China in the data economy, aims to propose/impose a *European way*, in which a hitherto unheard-of balance should distinguish between maximum use of data for the economic development of the Single Market on the one hand, and very high ethical, privacy, safety, and security standards on the other.

The major innovation proposed with the European strategy is the creation of thematic *data spaces*. The expansion of the Digital Single Market depends on the possibility of circulating data and extracting value, innovation, and benefits for the community from it. The European Commission proposes to bring about this effective change of gear with a system of data *pools* divided into thematic areas so that each sector can find suitable rules and individual spaces can at the same time communicate with each other to maximise the flow of data, with data silo limits being overcome.

Therefore, the European Union is preparing to create a large area of data localisation and exchange. This perspective introduces another issue that is far from easy to solve: the governance of cross-border data flows within the European Union.

As clarified by Recital 5 of the GDPR:

> The economic and social integration resulting from the functioning of the internal market has led to a considerable increase in cross-border flows of personal data and thus also in the amount of personal data exchanged, throughout the Union, between public and private actors, including natural persons, associations and undertakings [...].

German law. The German trustee and the data subject will be able to access the data, whereas Microsoft will only be able to do so in limited cases under the contract.

82 European Commission, *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 final, 19 February 2020, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:66:FIN.

The same applies to non-personal data flows, to which the oft-quoted Regulation 2018/1807 FFD is entirely dedicated, whose Recital 10 eloquently states:

> Under Regulation (EU) 2016/679, Member States may not restrict or prohibit the free movement of personal data within the Union on grounds relating to the protection of individuals with regard to the processing of personal data. This Regulation establishes the same principle of free movement within the Union for non-personal data [...] Regulation (EU) 2016/679 and this Regulation provide a coherent set of rules governing the free movement of different data types [...][83].

Therefore, the combined provisions of these two Regulations outline a model for the legal regulation of data exchanges between the Member States, which is an essential prerequisite for the development of a data economy in the European area.

The reluctance of Member States to consider services offered and located in other European States as part of a single legal area, combined with excessive protectionism[84], has led to a division of national databases into watertight compartments. This division has clearly weakened the EU's position in the global economy to date.

To counter this trend, the Union is committed to strengthening the common vision that is more necessary than ever for the maintenance and development of the Digital Single Market. The choice of opposing national location policies and supporting the opening up of flows between States is a good one because it is necessary to implement a data-driven economy. Certainly, enhancing trust with regard to data processing methods and clearly identifying chains of responsibility can help increase trust and, thus, cross-border data flows[85].

However, although the issue of trust is of primary importance, there is a strictly legal fact that seems to be the main cause of this system dysfunction, namely the regulatory fragmentation that still significantly differentiates data processing rules.

---

83 Article 4 of the FFD Regulation prohibits States from imposing location requirements that require processing on the territory of the State or hinder processing in another Member State.

84 COPASIR, expressing concern about malicious uses of data stored outside Italy, has explicitly referred to "*European and international actors*" who might be interested in the information collected; this perhaps suggests a lack of vision in terms of a common European data space.

85 Recital 7 of the GDPR refers to the importance of "*creating the trust that will allow the digital economy to develop throughout the internal market*". Franco Pizzetti defines it as the principle of trust, "*which must be taken as the basic interpretative criterion and as the ultimate objective that also justifies the close connection made by Article 1 GDPR between the implementation of the fundamental right to data protection and the need to guarantee its free movement*", in PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, 2018, p. 170.

This situation has been well highlighted recently in the report on the two years of implementation of the GDPR[86]. In it, the Commission criticises how complex it is to develop cross-border economic/commercial activities, relating in particular to technology, innovation, and cybersecurity[87], in the face of still evident differences in national legislation on aspects of great practical importance for companies, such as the consent of minors for information society services[88] and the system for processing particular categories of data.

Moreover, the Commission took the opportunity to call on Member States to take a "pan-European approach" and to coordinate more closely to avoid fragmentation when making recommendations for the technological management of the Covid-19 pandemic, with particular reference to the management of situations of the cross-border spread of the infection[89].

Returning to the data spaces strategy, this thematic subdivision should help overcome the fragmentation thus described by facilitating sharing of homogeneous personal and non-personal data within areas regulated by common rules developed for those spaces. In the words of the Commission: "*Such spaces aim at overcoming legal and technical barriers to data sharing across organisations, by combining the necessary tools and infrastructures and addressing issues of trust, for example, by way of common rules developed for the space*[90]".

The Communication, being a programme document, does not offer specific indications on the steps to be taken to implement this new European data storage and sharing model. Significantly, however, investment initiatives for a high-impact project on European data spaces and federated cloud infrastructures are announced for the 2021-2027 period.

In outlining the main features of the Strategy, the Commission takes the pragmatic stance of welcoming initiatives by the Member States for the creation of

86 European Commission, *Communication from the Commission to the European Parliament and the Council COM(2020) 264 final* "*Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation*" available at https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf.

87 See Ibid p. 7.

88 The GDPR allows the States to establish an age lower than sixteen (an opportunity taken, for instance, by Italy, which lowered the threshold to fourteen with Article 2 quinquies of the revised Privacy Code).

89 See European Commission, *COMMISSION RECOMMENDATION (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518&from=EN.

90 European Commission, *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*" cit. p. 16.

common infrastructures and announcing its willingness to draw up memoranda of understanding to facilitate the integration of these initiatives into the European project[91].

Given the "high-level" content of the document, it is worth noting the explicit reference to the Franco-German GAIA-X project, which we mentioned in the introduction[92].

We shall now briefly outline the main features of the project.

GAIA-X was the brainchild of the German government, but France soon became a partner, and the initiative was then presented to the rest of the EU countries at a launch conference on 4 June 2020. Once created, GAIA-X will be a digital infrastructure "*made in Europe*[93]". Its conception and progressive development are the results of the collaboration of more than three hundred public and private partners[94].

As far as we understand from reading the documents published at the project launch, GAIA-X will be a link module between national cloud and edge computing infrastructures. As in the case of infrastructures, it is also planned that GAIA-X will be regulated based on principles, rules, and standards already applied in the European Union[95].

The infrastructure will be open to participation by public and private actors that comply with what could be defined as the GAIA-X *acquis*, i.e., the set of "European" legal principles and rules and technical regulations that the initiative has adopted and which it plans to enhance with the progressive development of new policies and standards.

This *acquis* includes data protection, transparency, trust, data sovereignty, and interoperability[96].

It is worth noting that the terms *data sovereignty* and *digital sovereignty*[97] are both used in GAIA-X. While digital sovereignty is defined as decisional power "*about how*

91 Ibid, p. 18.
92 See Supra para. 1.
93 *GAIA-X: The European project kicks off the next phase on 04/06/2020*, available at https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=13, p. 2.
94 These include Google Germany GmbH.
95 On portability, interoperability, the interconnection between infrastructures, applications, data.
96 The *GAIA-X* document: *Policy Rules and Architecture of Standards*, 04/06/2020, available at https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-policy-rules-and-architecture-of-standards.pdf?__blob=publicationFile&v=4 recalling the Franco-German position identifies them as *1. European data protection 2. Openness, reversibility, and transparency 3. Authenticity and trust 4. Digital sovereignty and self-determination 5. Free market access and European value creation 6. Modularity and interoperability 7. Federation of infrastructure.*
97 *GAIA-X: Technical Architecture*, June 2020, available at https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=6, p. 3.

digital processes, infrastructures and the movement of data are structured, built and managed", *data* sovereignty is presented as a particular aspect of digital sovereignty, consisting of the data owner's full control over the location and use of data. Data sovereignty would thus be the first step towards full digital sovereignty.

The aim repeatedly referred to in the documentation released at the project's launch is to create a European ecosystem for the development of the data *economy*[98]. GAIA-X acts as a facilitator for developing the European data market[99]. In the GAIA-X ecosystem, businesses and public administrations should make the most of the potential of data by creating ever better services for citizens and business development for companies — all within the jurisdiction of at least one European country.

GAIA-X seems to be able to offer a viable — though yet largely unbuilt — alternative to the EU's dependence on global technology giants. Such an ecosystem could meet the demand for protecting citizens/users' rights and foster the development of the data economy at truly competitive levels. It could finally guarantee the digital sovereignty of the EU Member States. However, some points will certainly have to be clarified in the implementation phases.

For example, it is worth pointing out that each provider joining the infrastructure will remain responsible for the service it provides[100]: "*GAIA-X is a federated system of autonomous providers [...]. In accordance with the shared responsibility model, each GAIA-X Participant is responsible for the service and data which is controlled by him*". The published documents also state that a consumer may legitimately require proof of the actual location of his/her data, as opposed to what is guaranteed by the provider.

Thus, without the hype of the project launch and the enthusiasm associated with full adherence to the European strategy, GAIA-X presents itself as a system linking national servers located within the territory of the Union. A network of mutual agreements will provide legal certainty that all participants in the GAIA-X project meet the same technical and value requirements. It is proposed that compliance with the GDPR

98 "*GAIA-X combines the technological and industrial strengths of EU industry, academia and the public sector to develop an ecosystem of data and infrastructure providers and a regulatory framework based on fundamental European values and standards. The initiative supports the target of the EU to become a global leader in innovation in the data economy and its data-driven applications as set out in the European data strategy*" , in the document *GAIA-X: Driver of digital innovation in Europe*, available at https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-driver-of-digital-innovation-in-europe.pdf?blob=publicationFile&v=8, p. 25.

99 Ibid, p. 39.

100 *GAIA-X: Technical Architecture*, June 2020, available at https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=6, p. 30.

be verified by using certifications and codes of conduct in accordance with Articles 40 and 42 of the European Regulation[101].

This reference appears to be particularly appropriate and strategic in terms of the system's efficiency and even more so in terms of the development and strengthening of the European digital space. In the GDPR system, the development of codes of conduct should contribute to the correct application of the Regulation in specific sectors[102]. At the same time, certifications, seals, and marks should demonstrate the GDPR compliance of processing operations carried out in the provision of products and services[103].

Article 40, regarding codes of conduct, provides that associations or other bodies representing controllers and processors must submit the draft code to the competent supervisory authority, i.e., that of the State where the applicants have their registered offices. If the activities take place entirely within the territory of the State in which the association is located, the competent authority may independently proceed to approve the code of conduct.

However, what is relevant to the matter at hand is the procedure laid down in paragraphs 7 et seq. of the same article concerning cases of cross-border data flows. Indeed, when the draft code of conduct relates to processing activities involving several Member States, the competent supervisory authority must, in accordance with the consistency mechanism, submit the draft to the European Data Protection Board (EDPB). The Committee will express an opinion, which will then be forwarded (subject to a positive GDPR compliance assessment) to the Commission. The latter will then give the code of conduct general validity throughout Union territory by means of an implementing act.

Certifications, marks, and seals may be issued, in accordance with Article 42, by supervisory authorities, certification bodies, or the European Committee (EDPB). The latter has the power to approve certification criteria that would then allow data controllers and processors to obtain a European seal. Again, it is the supervisory authorities that identify the certification criteria. The Commission has the power, under

101 Ibid, p. 32.

102 Recital 99 of the GDPR specifies that codes of conduct should facilitate the application of the Regulation "*taking account of the specific characteristics of processing carried out in certain sectors and the specific needs of micro, small and medium enterprises*".

103 See Recital 100 of the GDPR, which states that certifications, seals and marks should enable data subjects to quickly assess the level of data protection offered by such products and services.

Article 43, to specify the requirements to be taken into account for certification and may lay down technical rules concerning these mechanisms and their promotion.

Therefore, as has been authoritatively pointed out (PIZZETTI, 2018, p. 175 ff), national supervisory authorities play a major role in the codes of conduct and certification. Going further, in some specific sectors, the GDPR provides for the intervention of the European Data Protection Board to monitor and coordinate the national authorities involved.

Once the reference ecosystem has been established, the bodies invested with regulatory and supervisory powers, working in coordination thanks to the cooperation and consistency mechanisms, will be able to help develop shared rules (including European codes of conduct) that will gradually lead to the creation of a legal space that is secure in terms of protection of fundamental rights and functional to the development of the data economy[104].

In support of this view, note that Article 64 para. 2 requires the European Committee to rule on matters of general application or relating to several Member States. This role appears to be of strategic importance for the progressive consolidation of European data governance. It is not by chance that Article 70 of the GDPR gives the EDPB the primary decisive task in ensuring the consistent application of the Regulation.

The abovementioned role of the Supervisory Authorities, the Commission and the European Data Protection Board in consolidating the Single Market becomes even more important in light of the option offered by the Regulation to data controllers and data processors not subject to the GDPR to adhere to codes of conduct and certifications in the context of personal data transfers to third countries or international organisations.

On closer inspection, the progressive construction of an agile and efficient regulatory apparatus could be the distinctive feature of the (big) data governance of the public sector through which the Union will be able to reaffirm (and protect) European sovereignty over data in the global digital chessboard.

104 In particular, the certifications, clearly designed to be used at European level, can be used by national authorities, the EDBD and the Commission to facilitate the circulation of data in the Union's digital space. Pizzetti emphasises the differences in the wording of Articles 40 and 42, which, far from being merely formal, show a distinct option for certificates of European validity. See *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit. p. 157 and p. 160.

REFERENCES

AIMIN, Q.; GUOSONG, S.; WENTONG, Z. Assessing China's cybersecurity law. *Computer Law & Security Review*, v. 34, n. 6, p. 1342-1354, 2018. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918303157.

AUSTIN, G. *Cybersecurity in China. The next wave*. Canberra: Springer, 2018.

BERTONI, F. Deepfake, ovvero Manipula et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda. *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, v. 20, n. 62, p. 11-28, 2018. Available at: https://www.mucchieditore.it/images/ExtraRiviste/ExtraCiberspazio122019.pdf.

CALZOLAIO, S. Digital (and privacy) by default. The constitutional identity of digital administration. *Journal of Constitutional History*, n. 31, p. 185-203, 2016.

CALZOLAIO, S. *Protezione dei dati personali*. Digesto delle discipline pubblicistiche. Turin: UTET, 2017.

COSTANZO, P. La democrazia digitale (precautions for use). *Diritto pubblico*, v. 1, p. 71-88, Jan./April, 2019. DOI https://doi.org/10.1438/93720.

DATA PROTECTION AUTHORITY. *Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"* – 13 February 2020. Rome, Garante per la protezione dei dati personali, [2020] Available at: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9283921.

D'ACQUISTO, G.; NALDI, M. *Big data e privacy by design*. Giappichelli: Turin, 2017.

DI FRANCESCO TORREGROSSA, M. *La competenza statale nel processo di digitalizzazione delle pubbliche amministrazioni*. Consulta Online Periodico Telematico, 2019. Available at: https://www.giurcost.org/contents/giurcost//studi/torregrossa1.pdf.

EUROPEAN COMMISSION. *Commission recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*. Official Journal of the European Union, [2020]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:32020H0518&from=EN.

EUROPEAN COMMISSION. *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"*. Brussels: COM(2020) 66 final, [2020]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:66:FIN.

EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council COM(2020) 264 final "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation"*. Brussels: SWD, [2020]. Available at: https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf.

GAIA-X: *Driver of digital innovation in Europe*. Featuring the next generation of data infrastructure. Federal Ministry for Economic Affairs and Energy (BMWi) Public Relations Division, Berlin: 2020. Available at: https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=8.

GAIA-X: *Policy Rules and Architecture of Standards*. Federal Ministry for Economic Affairs and Energy (BMWi) Public Relations Division, Berlin: 2020. Available at: https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-policy-rules-and-architecture-of-standards.pdf?__blob=publicationFile&v=4.

GAIA-X: Technical Architecture. Featuring the next generation of data infrastructure. Federal Ministry for Economic Affairs and Energy (BMWi) Public Relations Division, Berlin: 2020. Available at: https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=6.

GAIA-X: The European project kicks off the next phase. Featuring the next generation of data infrastructure. Federal Ministry for Economic Affairs and Energy (BMWi) Public Relations Division, Berlin: 2020. Available at: https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=13.

GENTILI, A. *La sovranità nei sistemi giuridici aperti*. Politica del diritto, v. 42, n. 2, p. 181-206, June 2011. DOI: https://doi.org/10.1437/35191.

GREENLEAF, G. *Asian data privacy laws*: *Trade & Human rights perspectives*. Oxford University Press, Oxford: 2014. DOI: https://doi.org/10.1093/acprof:oso/9780199679669.001.0001.

HUANG, L.; ILAN, D.; MOONEY CARROL, K.; ZHOU, Z. *Understanding the impact of China's far-reaching new cybersecurity law*. Intellectual Property & Technology Law Journal, v. 30, n. 2, February 2018.

ITALIAN DATA PROTECTION AUTHORITY. *Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro data-driven per l'emergenza COVID-19, de 07 de abril de 2020*. Roma, Garante per la protezione dei dati personali, [2020]. Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316821.

LINDSAY, J. R.; CHEUNG, T. M.; REVERON, D. S. *China and cybersecurity espionage, strategy, and politics in the digital domain*. Oxford University Press, Oxford: 2015.

MARKZAR, B.; SCOTT-RAILTON, J. Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings. *The citizen lab*, Toronto, 3 April 2020. Available at: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/.

MASUCCI, A. Digitalizzazione dell'amministrazione e servizi pubblici online. Lineamenti del disegno normativo. *Diritto Pubblico*, v. 1, p. 117-152, January-April 2019. DOI: https://doi.org/10.1438/93722.

PARLIAMENTARY COMMITTEE FOR THE SECURITY OF THE REPUBLIC (COPASIR), *Report on the security profiles of the Covid-19 alert system provided for in Article 6 of Decree Law No 28 of 30 April 2020*. Roma, Camera dei deputati, [2020]. Available at: http://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/002/INTERO.pdf.

PERSONAL DATA PROTECTION AUTHORITY. *Remote criminal trial: letter by the President of the Personal Data Protection Authority, Antonello Soro, to the Minister of Justice, Alfonso Bonafede*, de 16 April 2020. Roma, Garante per la protezione dei dati personali, [2020]. Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316889.

PIZZETTI, F. *Intelligenza artificiale, protezione dei dati personali e regolazione*. G. Giappichelli Editore: Turin, 2018.

POLLICINO, O. "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. *Federalismi.it*, n. 19, p. 1-15, October 2019. Available at: https://www.federalismi.it/nv14/editoriale.cfm?eid=533.

RUOTOLO, G. M. I dati non personali: l'emersione dei big data nel diritto dell'Unione europea. *Studi sull'integrazione europea*, n. 1, p. 97-116, jan. 2018.

SCIACCHITANO, F. Disciplina e utilizzo degli Open Data in Italia. *Medialaws*, p. 1-34, 2018. Available at: https://www.medialaws.eu/wp-content/uploads/2019/05/20.-Sciacchitano.pdf.

SCHWARTZ, P. M. Legal access to the global cloud. *Columbia Law Review*, v. 118, n. 6, p. 1681-1762, 2018. Available at: https://www.columbialawreview.org/wp-content/uploads/2018/10/Schwartz-LEGAL_ACCESS_TO_THE_GLOBAL_CLOUD.pdf.

SIMONCINI, A.; SUWEIS, S. Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale. *Rivista di filosofia del diritto*, v. 8, p. 87-106, June 2019. DOI: https://doi.org/10.4477/93368.