ISTITUTO ITALIANO
PER LA PRIVACY E LA
VALORIZZAZIONE DEI DATI

THE "TEMPTATIONS" OF THE EUROPEAN AND NATIONAL CLOUD: AMID POLITICAL SIMPLIFICATION AND LEGAL CRITICISM

25 September 2020

A study by Luca Bolognini* and Enrico Pelino**

The Italian Institute for Privacy and Data Valorisation

Table of contents

Abstract

The race to create local cloud solutions has become a constant in the digital development programs of member States. Italy is promoting the establishment of the so-called "national cloud", and Germany and France have been working for some time on the Gaia-X project. At European level, the development of cloud computing is taking a strategic role, at least for the immediate future. The declared objective is to free us from solutions that today are almost entirely dependent on infrastructures made available by international providers. Contributing to the debate - more by superimposition than composition - there are broadly geopolitical motivations, aspirations to global technological predominance and concerns associated with personal data protection for third party interference due to the extraterritorial application of foreign legislation. The recent "Schrems II" ruling by the Court of Justice of the European Union, and previously, but with less impact in the broader public, the results of the joint EDPB (European Data Protection Board)-EDPS (European Data Protection Supervisor) study on the United States' Cloud Act, have forced the question of the international acquisition of personal data flows (and non-personal, we may add) and the associated assurances.

This paper intends to offer an analysis of the subject, aimed above all at unravelling the multiple levels of the questions raised, which touch not only on legal but on political matters and give an initial, reasoned census of the various bodies of applicable law. Above and beyond hard-hitting declarations, we need to determine to what point the independence of a local European cloud is effectively possible or desirable compared to non-EU providers and, in more concrete terms, to what point an autonomous solution is economically and technically practicable in terms of services that are essential for the States, and that enable the exercise of other fundamental rights and freedoms, for individuals, and therefore must not be susceptible to impairment or interruption. We also have to understand to what point it would be opportune in terms of security, even if this, at first glance, may seem counter-intuitive. In this sense, at least in the overall assessment, we have to consider the high levels of service stability and the existence of high-tech measures to contrast *cybercrime*

that the major international providers can ensure, levels it would be inadvisable to forgo if it were possible to keep the benefits, thereby significantly reducing the associated risks. Indeed, the protection of processed data from external interference must also be measured on a different, but nonetheless significant, level to that of any potential "extraterritorial" threat, represented by criminal activity and security breaches. Another factor that must be considered is the availability of solutions, already entirely actual and "in the hands" of users, which offer immediate protection, such as encryption or the segregation of strategic data sets. In other words, if there are possible measures that significantly reduce the extraterritorial risk and that retain the advantages in terms of contrasting *cybercrime*, these must be duly included in the overall assessment.

Our analysis will also shed light on inconsistencies in terms of data protection within the European Union, and misalignments between national efforts toward localization and the principle of the free circulation of data. In short, we intend to offer a more articulate, less obvious outline of the subjects we are dealing with, which cannot be reduced (if not at the cost of excessive simplification) to the simple contraposition of E.U. *versus* non-EU, but which reveal lateral synergies and joint misalignments on fronts apparently united; rather, it would be better to think in terms of the creation of a shared ecosystem that draws the most significant advantage from the solutions available today and acknowledges the need to adopt concrete forms of protection. This does not in any way mean evading the serious, but not immediately solvable extraterritorial questions, but preferably using them, if anything, as a mechanism for obtaining a critical reconsideration of the shortcomings and lack of legal harmonization that emerge even within the European Union. Nor does it mean embarking on a path toward domestic solutions that offer little, or at least less protection than those currently available, but instead maintaining high levels of protection against unlawful activity through more advanced technological solutions, and at the same time identifying legal instruments which assure greater national control of the infrastructures and data, and reduce risk to a legally acceptable level.

The context - Toward the implementation of national clouds

In an interview in the daily "Il Sole 24 Ore" in February 2020, following on from anticipations of the previous November[1], the Italian Minister for Innovation, Paola Pisano announced the start of a project, currently at the development stage, to create a national cloud that would most likely be managed through a joint venture between State and private sector providers with minority shareholdings, chosen through an open tender procedure. The declared objective referred above all to considerations of a geopolitical nature: to prevent the interruption of service or external interference due to international tensions, even if not involving Italy or the European Union but which could affect global providers of cloud technology or the physical infrastructures themselves[2]. The proposed model does not envisage the management of all public information but postulates a selection upstream. In specific terms, according to the declarations: "*the Pole would only handle critical data concerning issues of national security, and would, in any case, be monitored by the various existing Supervisory Authorities, according to their respective remits".*

On 23 June 2020 during his annual report to Parliament and the Government, the *former* President of the Italian Data Protection Authority (Autorità Garante per la protezione dei dati personali), Antonello Soro, in turn, raised the purely political question of the creation of a State cloud infrastructure, in connection with national security objectives and digital sovereignty. This marked a further institutional convergence on these matters. In particular, his reasoning drew on an examination of the risks associated with *data breaches* or least certain types of breach. Indeed, the President pointed out that: "*The implications, in terms of national security, of certain types of data breach also demonstrate how the close*

1 F. Me., *Pisano: "We need an Italian cloud to protect against geopolitical threats"*, in the *Corriere delle comunicazioni – CorCom*, 27 November 2019, https://www.corrierecomunicazioni.it/digital-economy/pisano-serve-un-cloud-italiano-contro-i-rischi-geopolitici.

2 F. Me., *Pisano: "A State-private sector joint venture for the national cloud"*, in *Corriere delle comunicazioni – CorCom*, 20 February 2020, https://www.corrierecomunicazioni.it/pa-digitale/pisano-joint-venture-stato-privati-per-il-cloud-nazionale/

dependence of network security on the organizations that manage the various hubs and 'channels' leads us to rethink the very concept of digital sovereignty.

And because of the de-localization of extremely significant activities, we ask Parliament and the Government whether they should invest in a public cloud infrastructure, with stringent protection requirements and adequate security for data of such importance.

In a scenario in which ICT technology has become - even more clearly in the light of the pandemic - the main infrastructure of each country, assuring adequate, sustainable regulation, independence from private powers and subjection to domestic jurisdiction is an objective we can no longer avoid" (see GPDP, Annual report 2019, President's speech, Web doc no. 9428327). As we can see, the report addresses two, not necessarily connected conceptual poles: information security and the applicable law, to which we will return later on,

Broadening our view in a *zoom-out* from Italy to the European Union, we cannot but notice the widespread development of initiatives aimed at creating local cloud infrastructures, confirming a marked, recognizable and shared political direction. The most visible of these initiatives is probably the pan-European "Gaia-X"[3] project, presented by the German government on 29 October 2019 and at present managed almost exclusively by Germany and France, which actually contemplates the participation of more than twenty large European groups mostly in the Telco and I.T. sectors[4]. In exactly the same way as the Italian national cloud project mentioned above, this platform does not exclude the participation of large international providers, in particular from the United States, provided they abide by a regulatory code[5].

3 See data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

4 These include the following, for example: Amadeus, Atos, Beckhoff, Bosch, BMW, DE-CIX, Deutsche Telekom, Docaposte, EDF, Fraunhofer, German Edge Cloud, Institut Mines Telecom, International Data Spaces Association, Orange, 3DS Outscale, OVHcloud, PlusServer, Safran, SAP, Scaleway, Siemens. See L. Tung, *Meet GAIA-X: This is Europe's bid to get cloud independence from US and China giants*, in *ZDNet*, 8 June 2020, *https://zd.net/3iq6qpk.*

5 See last art.

At present, the relationship between the Italian project and the Franco-German platform currently under development is not entirely clear, particularly as regards whether, and on what terms, Italy intends to take part in it, above and beyond general manifestations of interest[6]; all the more if we consider the fact that the initial choices of set-up, without coordination between the two models, could lead to diverging solutions. To this regard, we would hope to see some clarification on the intentions and on any reasons for self-exclusion from a project that is at a more advanced stage than the Italian one, and for setting such an ambitious objective requiring significant investments both economic and technological. Although legitimate, the choice to 'go it alone' is indeed a weighty decision with substantial consequences; hence it would only be fair to share the reasoning behind it.

Broadening our view in a further *zoom-out*, we can see that the directives for the creation of European cloud platforms ideally fall within the common framework of initiatives programmed by the European Commission, to which they all must adhere. Hence they should be created as parts of an ecosystem developed according to the strategies defined at European institutional level. Precisely on this aspect, it is worth mentioning the document entitled *A European strategy for data*[7]. Key elements of such strategy will be also the creation of a European federation of cloud infrastructures and services, of a European marketplace for cloud services, of a governance framework and an E.U. Cloud Rulebook[8].

This is the general context of our analysis. It could be enriched, mentioning similar projects, but we feel that the outline given so far should suffice for our purposes.

6 Luigi Garofalo, *Pisano: "Define the rules for the European cloud, but it is not possible to exclude Big Tech from the PA"*, in *Key4Biz.it*, 5 August 2020, *key4biz.it/pisano-definire-le-regole-per-il-cloud-europeo-ma-non-e-possibile-escludere-le-big-tech-dalla-pa/317590*.

7 European Commission, 19 February 2020, COM (2020) 66 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 _20_283.

8 See, for example, https://ec.europa.eu/digital-single-market/en/cloud.

The complex coordination of sources

First, we should clarify the fact that the subjects we are dealing with do not make for easy reading. Indeed, they don't just concern the strictly juridical field, but the sphere of political objectives as well, touching on the reciprocal interactions and limitations of both spheres. In various ways and to various degrees, they also involve the sphere of legal rights, at least those listed below:

- General Data Protection Regulation – reg. (E.U.) 2016/679 (so-called "GDPR"), dir. 2002/58 (so-called "EPrivacy Directive"), and National supplementing/implementing laws;
- Discipline regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data-dir. (E.U.) 2016/680, and National implementing laws;
- Extra E.U. laws concerning National Security and foreign intelligence: in particular, in USA, the Section 702 FISA;
- E-evidence law: Cloud Act USA and European draft regulation COM / 2018/225 final - 2018/0108 and draft directive COM / 2018/226 final - 2018/0107;
- European Regulation on free flow of non personal data, reg. (E.U.) 2018/1807;
- European law concerning measures for a high common level of security of network and information systems across the Union - dir. (E.U.) 2016/1148, and National implementing laws;
- European and National laws concerning digital Public Administration.

A complete study of the reciprocal implications of the various bodies of law would be far too complex and premature at this stage: the aim of this paper is not to give a complete

analysis of the interactions between the various regulations, but that of providing an efficient tool able to prepare the field for a more articulate debate. The main focus will therefore be on the protection of personal data, in keeping with the vocation of the institute. This is a very broad-reaching area of law, if we consider the "osculant" nature of personal data and the dynamism inherent in the concrete application of the concept of re-identification. In other words, unless we can be absolutely certain that the data sets being processed are not personal, to be prudent we should nevertheless consider them as personal, and consequently apply the most rigorous standards. It is also worth mentioning that the Court of Justice of the European Union recently intervened on these matters, through the so-called "Schrems II" ruling, namely CJEU ruling C-311/18 dated 16 July 2020, the implications of which cannot be ignored in a study on local and global cloud computing. Therefore we will be approaching the subject considering it above all from the point of view of compliance with the legislation on the protection of personal data.

The dependence of the P.A. on non-EU providers

At present, the world market for cloud infrastructures is dominated by five large groups, four of which (Amazon, Microsoft, Google and IBM) based in the United States, and the fifth, Alibaba, in China. The remaining market share is distributed among a number of other groups, most of which based in North America (e.g. Cisco Systems, Salesforce and Oracle) with the exception of a few European groups established in the EU[9]. This situation depends principally - as far as we can see - on market dynamics and free competition, economic capacity and investments sustained for the implementation of the infrastructures, research and development, and the initial technological assets of the providers. This in itself is significant, because any government investments directed toward the construction of a

9 For a more in-depth analysis, see, L. Dignan, *Top cloud providers in 2020: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players*, in *ZDNet*, 11 May 2020, https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/

national cloud cannot but take account of economic factors and sustainability over time, and cannot ignore the need to meet the efficiency parameters the market demands.

The current situation in terms of the offer of cloud solutions thus constitutes an element of fact, to be taken as such. It leads to a number of precise legal implications. For example, for some time now Italy has been applying a "**cloud first**" strategy, confirmed by the latest Three-Year IT Plan 2019 – 2021, requiring the Public Administration to define new projects and develop new services through cloud solutions, preferring in particular the SaaS model above any other technical solution and, more generally, to use cloud solutions with the intention of *"acquiring new ICT solutions and services for the implementation of a new project or new services destined for citizens, businesses or users within the P.A. itself*"[10].

The rationale is evident and fully acceptable: the cloud is the most affirmed standard and gives recognizable advantages in terms of efficiency, scalability, economy and resilience with respect to traditional I.T. models like *housing* and *hosting*[11].

Consequently, the combination of these two elements, namely the current market situation and the "cloud first" principle, means that for its essential operations, and at least in the scope of public clouds, the Public Administration tends to depend largely on the previously mentioned international providers[12], whether directly or indirectly through intermediaries. This is precisely the scenario in which the project to establish a national cloud is set.

10 See *The cloud model of the PA*, 13 February 2020, § 4.1, in https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/index.html

11 It is worth noting that this approach has been fully approved at European Union level, see European Commission, *A European strategy for data*, which, in the context of an as yet insufficient adoption of cloud platforms by public administrations of the member States in general, reads as follows: "*Specifically, cloud uptake in the European public sector is low. This may lead to less efficient digital public services, not only because of the clear potential to cut IT costs by cloud adoption, but also because governments need the scalability of cloud computing to deploy technologies like Artificial Intelligence.*".

12 According to the information provided by the Italian Minister for Innovation "*Today we source 80% of cloud resources from outside the EU*", see Fabio Savelli, The battle for (our) digital sovereignty: the race to national clouds, in Corriere della sera, online issue, 6 July 2020, https://bit.ly/32nyAf3

Similar considerations are expressed in the previously quoted European Commission *European strategy for data*, in particular: "*EU-based cloud providers have only a small share of the cloud market, which makes the E.U. highly dependent on external providers, vulnerable to external data threats and subject to a loss of investment potential for the European digital industry in the data processing market*".

Having laid out the essential points of the subject, we have to consider whether the actual situation of dependence on large, non-national providers could, in reality, represent a risk factor, and to what point and what reason; then in what way the creation of domestic solutions is capable of mitigating such risk, and in any case whether and to what degree a number of the problems generally raised in the public debate can be resolved through a more detailed examination.

The triad approach - confidentiality, availability, integrity (CIA triad)

In order to identify the type of risk and to study the necessary mitigation methods, the most immediate and consolidated approach seems to be the one offered by the classic triad model, which interprets risk on the basis of three parameters: loss of data confidentiality, integrity and availability, and eventually the cumulative effect of all three.

This model has the advantage of being applicable to both personal and non-personal data. More detailed applications of the model could include attributing numerical coefficients to the various risk factors, to estimate the probability and level of threat, but for the time being it is somewhat difficult to identify elements suitable for the specific and highly peculiar reference context that permit their determination.

Risks associated with *data breach* incidents

One of the first issues to tackle, above all, to give due consideration to the institution that expressed them, regarding the relationship between *data breach* incidents and national security/digital sovereignty. The reference to the CIA triad here is quite obvious, given that (personal[13]) data infringements, by definition, consist of events concerning the destruction, loss, modification, disclosure and unauthorized access (see art. 4, para. 1, no. 12 GDPR).

The core concept of the notion of *data breach* is the occurrence of an infringement of data or organizational security. However, for this same reason the relationship postulated by the President of the Italian Data Protection Authority (Autorità Garante per la protezione dei dati personali), between nationalization of the infrastructure and data breach events, is not immediately clear, at least not without some further elements and clarification. In other words, in the final analysis, security incidents originate from malicious or negligent behaviour and so are usually due to the quality of the organizational or technological measures adopted, the continual updating of standards and the conduction of periodic *audits*; in short a series of regulations placed on a level completely independent and lateral to questions of the national or international nature of the provider. The rules of cybersecurity, once defined, implemented and guaranteed, remain such at any level.

It is true that our opening considerations also contain references to jurisdiction, which, if we understand them correctly, could allude to difficulties in communication and collaboration in relations between non-EU providers and European control Authorities and/or insufficient response toward the interested parties, in other words, to the effective observance of the provisions of the GDPR (E.U. reg. 2016/679). However, we are not aware of sanctions imposed by the Italian Data Protection Authority clearly correlated with such situations; so, any argument aimed at more precisely identifying the reasons for dissatisfaction and the connection with the call to construct a national cloud remains merely

13 The considerations expressed can nevertheless be extended to the processing of non-personal data.

hypothetical, and unfortunately cannot count on any concrete foundation for its development.

The extraterritorial application of third country legislation

The subject of jurisdiction and the application of the third country legislation is, in any case, a central matter and needs further analysis, regardless of the considerations expressed in the previous paragraph. From a certain point of view this - at least in legal rather than political terms - is the very core of the question, as shown by the importance it normally takes in the debate developing around cloud platforms developed by non-EU providers.

We can, in very general terms, split the problems that could arise into two macro-categories:

- problems connected with data processing by foreign Authorities for *intelligence*, defence and national security purposes, in accordance with the civil rights legislation of the third country;
- problems associated with requests for personal data from the judicial/administrative Authorities of third countries.

This distinction is merely indicative, and some degree of overlap is possible in the sense that even processing for *intelligence* purposes may include phases of legal verification, even if through special courts[14].

14 For example, the *Foreign Intelligence Surveillance Court* (FISC) with respect to the FISA.

Intelligence, defence and national security of third party countries

Approaching the question in order, the Schrems II ruling was constructed on the basis of the first macro-category (and likewise the preceding Schrems I ruling, namely CJEU C-363/14 dated 6 October 2015. Naturally, in this sense, our examination of United States legislation is only a practical *case study*, given that it is already the subject of more complete analyses, but it goes without saying that the same methodology must be applied and extended to any other third Country, so for example to China and Chinese legislation, with regard to the question of Chinese cloud platforms or the use of Chinese infrastructures[15].

With regard to the United States' legislative context, the E.U. Court of Justice in the ruling we are talking about dwells above all on two bodies of law, *Section* 702 of the Foreign Intelligence Surveillance Act (FISA) and E.O. 12333 (see cited ruling, § 60 et seq.). At this point, it is worth quoting some excerpts from this ruling, for a clearer contextualization.

In the first provision, the European judge concludes, "*Section 702 of the FISA permits the Attorney General and the Director of National Intelligence to authorize jointly, following FISC approval, the surveillance of individuals who are not United States citizens located outside the United States in order to obtain 'foreign intelligence information', and provides, inter alia, the basis for the PRISM and UPSTREAM surveillance programmes. In the context of the PRISM program, Internet service providers are required, according to the findings of that court, to supply the NSA with all communications to and from a 'selector', some of which are also transmitted to the FBI and the Central Intelligence Agency (CIA). As regards the UPSTREAM program, that court found that, in the context of that program, telecommunications undertakings operating the 'backbone' of the Internet - that is to say,*

15 See the recent problems raised by the Commission in *A European strategy for data*: "*China has a combination of government surveillance with a strong control of Big Tech companies over massive amounts of data without sufficient safeguards for individuals.*". More in general: "*Service providers operating in the EU may also be subject to legislation of third countries, which presents the risk that data of EU citizens and businesses are accessed by third country jurisdictions that are in contradiction with the EU's data protection framework*".

the network of cables, switches and routers - are required to allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to or about a non-US national associated with a 'selector'. Under that program, the NSA has, according to the findings of that court, access both to the metadata and to the content of the communications concerned." (§§ 61-62).

The Court went on to add: "*(this) allows the NSA to access data 'in transit' to the United States, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA. It adds that activities conducted pursuant to EO 12333 are not governed by statute.*" (§ 63).

In general terms, American cloud technology providers can be considered subject to the cited provision of the FISA in that they are "*electronic communication service providers*".

The type of risk identified on the basis of the CIA triad is essentially that of the loss of confidentiality, with the consequences this has for data subjects, considering the scope of intelligence and, according to the case, anti-terrorism.

With respect to the cited sources, the Schrems II ruling considered that this surveillance was massive and that the level of protection for European citizens deriving from this legislative framework was incompatible with the European Charter of Human Rights, and with the GDPR.

Seeing the legislative context in this light, we have to ask ourselves whether it is only the transfer of data to the United States that is in contrast with the protection structure in effect in the Union and thus whether the localization of cloud infrastructures in the E.U. could be a remedy. In this respect, in a positive sense it is worth noting that for some time now a number of non-European providers have created *data centres* in the European Union and guarantee, often through controlled companies, the circulation of information exclusively within the territorial "bubble" of the Union: in other words, there is already a "European" cloud, even if not managed by European businesses or with member State

participation. Nevertheless, we also have to understand whether the E.U. affiliates of American cloud providers are subject to *Section* 702 FISA, and so whether localization in Europe, in this respect, substantially loses relevance.

In any case, we have to consider that the responsibility for ensuring conformity of the platform to the GDPR and the EU Charter of fundamental rights - namely, with respect to the hypothesis under examination, the absence of information lows without legal basis and the requirement of lawfulness toward the American authorities - weighs above all precisely on the E.U. affiliates of the aforementioned providers. It is indeed clear that, on one hand, the application of art. 3 GDPR and on the other the full inclusion of processing for national security reasons of the third Country fall within the scope of the Regulation[16]. This responsibility could thus be well defined in the request for suitable guarantees and requests for legal clarification on the part of clients entrusting data to clouds, clearly privileging providers able to offer such guarantees.

From a completely different standpoint, we also have to consider that a practical measure for containing the risk of application of *Section* 702 FISA can be found in the use of robust **encryption** techniques, directly and independently activated by cloud service users. In this way – with the exception of unknown vulnerabilities in the protocols or the use of quantum computers for decryption – it is possible to contrast the risk of loss of data *confidentiality*, namely the risk factor recognized in the application of the CIA triad, by the upstream placement (that is to say at client/user level) of the level of access to the unencrypted information. Not by chance, encryption constitutes a measure considered valid in the European guidelines on *data breach*, precisely in relation to the risk of loss of

16 See CJEU *cit.* § 81: "*In that regard, it should be made clear at the outset that the rule in Article 4 (2) TEU, according to which, within the European Union, national security remains the sole responsibility of each Member State, concerns Member States of the European Union only. That rule is therefore irrelevant, in the present case, for the purposes of interpreting Article 2 (1) and Article 2 (2) (a), (b) and (d) of the GDPR.*".

confidentiality[17]. The same considerations, therefore, cannot but be transposed into the context under examination here.

Instead, the localization of cloud infrastructures in the territory of the European Union only offers protection to the degree it is accompanied by effective forms of control over the continuity of the cloud by the member States, in the vent of (potential) interruptions of service associated, with hypothetical international tensions. This scenario is obviously different from the previously mentioned questions of surveillance for intelligence purposes and does not seem to be formulated with respect to any specific third Country, but examined as a mere geopolitical eventuality. In this case, the type of risk considered in terms of a CIA triad is that of the availability of data and, potentially (according to the case), likewise its integrity, but this risk can be contained through the physical localization of the infrastructures in Europe.

Request moved by the third Country judicial Authorities

Moving on to the second macro-category of problems associated with the application of third Country legislation, this concerns orders to produce data issued by foreign judicial or administrative Authorities. In this case, too, the richest case study for a legal analysis is given by the North American legislative context, and here too the principle that the analysis must naturally be conducted in general terms with respect to any requesting authority or any third Country is equally valid. The type of risk, according to the CIA triad, is that of the loss of data confidentiality.

From a legislative standpoint, we have to remember that wherever personal data is processed, as a necessary condition for the lawfulness of its communication, art. 48 of the GDPR requires the presence of "*an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member*

17 See WP29/EDPB, *Guidelines on Personal Data Breach Notification Under Regulation 2016/679*, WP250 rev. 01.

State". An agreement of this kind was signed in 2003[18] (but in a context in part unsatisfactory with respect to a number of the contemporary requirements of judicial cooperation). In concrete terms, apart from the aforementioned bilateral agreement, a direct court order was issued during the dispute between Microsoft Ireland and the United States (Warrant Case) in 2016, which concerned a judicial order for access to data stored on an Irish server, formulated by the American judicial Authorities and opposed in court by the European affiliate of the American company.

Subsequently, on 23 March 2018, the Cloud Act came into effect, which amended the Stored Communications Act (SCA) of 1986. The new legislation applies to providers who fall under U.S. law and, according to a preliminary study conducted in 2019 by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), the new agreement is likely to override the existing bilateral agreement between the European Union and the United States[19]. Hence in this respect, the Cloud Act poses a problem to art. 48 of the GDPR and would require a new agreement between the member States and/or the European Union and the USA in such circumstances (an instrument, among others, contemplated by the Cloud Act itself).

The study also highlights that the principal element of the Act in question is the irrelevance of the place in which the data under the order is stored. In this respect, any decisions to localize data in the European Union would be ineffective against the scope of the legislation, if the cloud service provider were a company that falls under U.S. law or an affiliate of that company.

18 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719(02)&from=EN.

19 See EDPB and EDPS, *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*, 10 July 2019, page 1: "*By choosing to create a legal avenue under US law for US law enforcement authorities to require disclosure of personal data directly from service providers who fall under US jurisdiction, irrespective of where the data is stored, the US Congress enacts into US law a practice of US governmental entities likely to bypass the Mutual legal assistance in criminal matters treaty (MLAT) in force between the European Union and the United States of America*".

In all truth, the territorial scope of the Cloud Act has juridical implications that have yet to be ascertained. For example, the joint study notes: "*Other questions regarding the scope of application of the US CLOUD Act remain to be resolved, (e.g. whether it applies to* ***E.U. operators*** *with some "presence" in the U.S., and how the concept of "control" is to be interpreted in practice, in particular with regard to* ***affiliated companies*** *of U.S. based companies, established in the E.U.)*"[20]. If this hypothesis found confirmation, the situation of a number of European providers would be comparable to that of American providers, due to the lack of substantial juridical differences.

Even in this case, the considerations previously formulated with regard to non-EU surveillance activities for intelligence purposes can be applied, namely that it is the responsibility of the provider potentially subject to the Cloud Act to give adequate guarantees with regard to compliance of the processing with the GDPR. From this perspective, the economic weight of the provider generally constitutes an element of reliability, since if opportunely valorized, this factor gives legal resilience to demands in contrast with art. 48 of the GDPR and other provisions of the European Regulation, whereas on the other hand, it is likely that subjects with little economic weight risk being overwhelmed.

This having been said, it is in any case necessary to contextualize the cases of data flows due to order by judicial or administrative authorities with respect to those linked with mass surveillance for *intelligence* purposes. The first case usually considers targeted, rather than exploratory orders, based on evidence and accompanied by the guarantee of ordinary process, albeit with all the protective limitations regarding non-US citizens before the U.S. courts.

As before, a means of contrasting the risk of loss of *confidentiality* of personal data subject to judicial or administrative orders can be found in the encryption of the data by the clients/users of the cloud service themselves.

20 Ibid. p. 2.

Lastly, we have to consider the concept of reciprocity. Indeed, for judicial activities and investigations the European judicial authorities have every interest in accessing electronic evidence stored by companies operating in the United States: just consider the *vulnus* that could derive with respect to investigations into organized crime. In other words, the question of judicial collaboration is intrinsically multilateral, and the risk posed by sudden interruptions should be assessed as a whole in the light of the potential loss of opportunities for cooperation. On this point, it is worth remembering that the European Union is currently establishing legislation on *e-evidence*, at present awaiting approval, and is starting specific negotiations with the United States[21] to establish a reciprocal cooperation agreement with the Cloud Act.

Two features emerging in the Italian national cloud project

Ultimately, the elements of uncertainty briefly analyzed in relation to surveillance for *intelligence* purposes, and administrative/judicial orders reveal their most critical aspect in questions of a jurisdictional nature, questions which regard the broad range of application of a number of regulatory acts in force outside the E.U. In real terms it is not easy to identify immediate solutions, given the evident impracticality of the idea of suddenly replacing providers with cutting-edge technology, firmly established on the market and who enable essential public services or in any case the exercise of fundamental rights and freedoms even for citizens of the European Union. At most, in the short term, we could study new legal forms for business structures eventually capable of escaping the scope of application

21 See EU Commission, *A European strategy for data*: "*While third country legislations like the US CLOUD Act are based on public policy reasons such as law enforcement access to data for criminal investigations, the application of foreign jurisdictions' legislation raises legitimate concerns for European businesses, citizens and public authorities over legal uncertainty and compliance with applicable EU law, such as data protection rules. The EU is acting to mitigate such concerns through mutually beneficial international cooperation, such as the proposed EU-US Agreement to facilitate cross border access to electronic evidence, alleviating the risk of conflict of laws and establishing clear safeguards for the data of EU citizens and companies . The EU is also working at the multilateral level, including in the context of the Council of Europe, to develop common rules on access to electronic evidence, based on a high level of protection of fundamental and procedural rights*".

of foreign legislation. Another pragmatic solution already considered is that of having clients/users adopt robust information encryption techniques, to render their data unintelligible to providers and hence the requesting third Country authorities as well.

Bringing the analysis back to the national cloud project, in the Italian case, it is worth noting that the model currently being developed by the government does not exclude the participation of large non-EU providers in the infrastructure. In this respect, as mentioned in the opening to this paper, it seems to be based on a strategically significant distribution of the information processed in the cloud, which would seem correct, and on the mere valorization of a spatial coordinate (national localization, to this regard, see also art. 35, para. 1, lett. a), L.D. no. 76 dated 16 July 2020, see later), but not on a jurisdictional coordinate as well (the foreign law applicable to the provider).

The reasons for involving non-EU providers seems to be substantially pragmatic and reflects the perceived difficulty in replacing the services already provided by other national solutions, as the declarations of the Minister for Innovation reveal with regard to the alignment of the new supply structure: "*Our strategy for the cloud and digital infrastructures cannot possibly ignore the current reality. For this reason, it envisages the use of solutions already existing in the Public Administration, and infrastructures that only foreign groups can provide*"[22]. What appears new in this is the legal "container" and the strengthened public control in decisional and management terms. At this time it is not possible to gauge whether and in what terms this new framework, both legal and structural, is able to mitigate the extraterritorial scope of the foreign jurisdiction, given that (and as opposed to the Gaia-X project) documents describing the specifics of the project have not been made public. Therefore our knowledge is limited to hints given by the Minister in interviews and declarations. Again, this makes it impossible to assess the real contribution of the new strategy in concrete terms.

22 See last cit. doc.

The provision of essential technological-infrastructural support by non-EU cloud providers up to this point is a self-evident fact and departs even from the need for the provider to have an establishment in Italy. To this regard, see art. 5, memo 3/2018 and art. 5, foreign memo 2/2018 issued by the Digital Italy Agency (AgID): "*In the case of a provider without any form of direct or indirect representation in Italy, upon notification by the proposing administration, the AgID acquires the information necessary for their qualification and can automatically initiate the procedure through the AgID platform established for that purpose, in the manner as published on the Cloud Italia site at the address: https://cloud.italia.it/*".

Conflicts between localization obligations and Euro-unitary legislation: the Italian example

On a different front, namely that of the legal relationship between national clouds (or localized solutions in general) and European Union legislation, there are a number of points demanding attention with respect to the *Free Flow of Non-Personal Data Regulation*. Article 2 of this Regulation applies to "*the processing of electronic data other than personal data in the Union, which is: (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union; or (b) carried out by a natural or legal person residing or having an establishment in the Union for its own needs.*". The term "users" is defined as "*a natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service*". So it would seem that the regulation also applies to the cloud services of the Public Administration.

With regard to Italian example, for the purposes of this necessarily summary analysis we will be considering the specific nature of the localization obligations established by art. 9, para. 2 DPCM 3 December 2013, on "*Technical regulations concerning data storage systems in accordance with articles 20, paragraphs 3 and 5-bis; 23-ter, paragraph 4; 43,*

paragraphs 1 and 3; 44, 44-bis and 71, paragraph 1, of the Digital administration code in pursuance of legislative decree no. 82 dated 2005", and the provisions of art. 33-*septies*, para. 1 L.D. No. 179 dated 8 October 2012, as amended by art. 35, para. 1, lett. a), L.D. no. 76 dated 16 July 2020.

Following the order as above, the first provision establishes: "*Without prejudice to the provisions of legislative decree no. 42 dated 22 January 2004 on the protection, by the Ministry of Cultural Heritage and Activities and Tourism, of the archives and documents of the State, the Regions and other territorial public bodies, organizations and institutions, for the supervision thereof by the Digital Italy Agency the data storage systems of the public administration and the storage systems of other accredited entities shall envisage the physical storage of data and back-up copies within the national territory and assure access to data at the establishment of the controller thereof and security measures in compliance with those established by this decree*".

The second provision reads: "*The President of the Council of Ministers promotes the development of a high-reliability infrastructure localized within the national territory for the rationalization and consolidation of the data processing centres (CED) defined by paragraph 2, for all public administrations*". The national infrastructure is designed to ensure a safe haven for migration to data processing centres of information lacking the security requirements established by the AgID, as envisaged by paragraph four of the article in question. Alternatively, the solution proposed by paragraph 4-*ter* could be adopted, or migration to CED compliant with the AgID requirements, or lastly, and of most interest to this paper, migration to cloud solutions in line with the AgID requirements. At this point, we find ourselves before a framework of possibilities constructed on a variety of alternatives.

Given that the overall formulation of the degree does not seem to imply the introduction of an obligation to national localization, in the precise sense of the term, before any further comment it would be useful to briefly reconstruct the regulatory framework introduced by the aforementioned (E.U.) reg. 2018/1807 on the *Free Flow of Non-Personal*

Data and the underlying *rationale*. The cornerstone of the European unitary discipline is art. 4, para. 1 of the Regulation in question, which explicitly forbids "data localization requirements", save for a number of exceptions (see next paragraph). *"Data localization requirements",* as clarified by art. 3, para. 1, no. 5), means *"Any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24 / E.U., which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State*".

The *rationale* is better clarified in the Recitals. For example, the second Recital states: "*Data value chains are built on different data activities: data creation and collection; data aggregation and organization; data processing; data analysis, marketing and distribution; use and re-use of data. The effective and efficient functioning of data processing is a fundamental building block in any data value chain. However, the effective and efficient functioning of data processing, and the development of the data economy in the Union, are hampered, in particular, by two types of obstacles to data mobility and to the internal market: data localization requirements put in place by Member States' authorities and vendor lock-in practices in the private sector.*". Similar considerations are developed in subsequent Recitals 3 and 4. Recital 6 (see also Recital 17) then explicitly associates the *cloud computing* sector with the two obstacles mentioned above, and further obstacles associated with juridical, contractual and technical problems which impose limitations (just as preceding Recital 5), evoking two orders of prejudice directly linked with such obstacles:

- freedom of competition recalled explicitly even in Recital 18;
- the progress of research and development.

In substantial terms - in a rough interpretation - mandatory localization is comparable, *mutatis mutandis*, to a sort of *vendor lock-in* of a public nature.

Here it is certainly worth quoting Recital 6, which clearly illustrates the *rationale* of the European unitary provisions: "*The combination of those obstacles has led to a lack of competition between cloud service providers in the Union, to various vendor lock-in issues, and to a serious lack of data mobility. Likewise, data-localization policies have undermined the ability of research and development companies to facilitate collaboration between firms, universities, and other research organizations with the aim of driving innovation*".

Recital 13 of (E.U.) reg. 2018/1807 invites public authorities and bodies governed by public law to "*refrain from making data localization restrictions when they make use of data processing services*".

This is made even clearer in Recital 18, which is worth quoting in its entirety: "*Data localization requirements represent a clear barrier to the free provision of data processing services across the Union and to the internal market. As such, they should be banned unless they are justified on grounds of public security, as defined by Union law, in particular within the meaning of Article 52 TFEU, and satisfy the principle of proportionality enshrined in Article 5 TEU. In order to give effect to the principle of free flow of non-personal data across borders, to ensure the swift removal of existing data localization requirements and to enable, for operational reasons, the processing of data in multiple locations across the Union, and since this Regulation provides for measures to ensure data availability for regulatory control purposes, Member States should only be able to invoke public security as a justification for data localization requirements*".

It is useful to note that pursuant to art. 4 para. 2 (see also Recital 20) member States are required to give immediate notice to the Commission of any project likely to introduce a new data localization requirement, or which alters an existing one, in compliance with articles 5-7, (E.U.) Directive 2015/1535. As for the requirements present prior to the regulation, these must be removed by 30 May 2021, as established by paragraph 3, unless with suitable justification subject to approval by the Commission.

Having thus summarised the essential lines of the regulatory framework introduced by (E.U.) Regulation 2018/1807, and reviewed the two national provisions mentioned in the opening, a number of grounded perplexities can be formulated regarding the compatibility of the first of them with the new European framework, with regard to art. 9, para. 2 DPCM 3 December 2013 on the storage of electronic documents. Then again, it is worth noting the existence of a convincing argument in the *opposite* sense, namely that art. 4.9, first sentence, of the AgID guideline on the formation, management and storage of electronic documents adopted pursuant to art. 71 of Leg. Dec. 82/2005 (the eGovernance Code, CAD), in the version prior to the critical observations of the European Commission,[23] contains formulations that substantially[24] follow those of the above DPCM, where the new formulation, transposing the Commission's observations, explicitly states: "*Without prejudice to the provisions of the Cultural Heritage Code, in observance of the principle of the free circulation of data within the European Union, we emphasize the requirement of storage service providers to keep and make available* ***the descriptions of the storage system*** [and no longer *"the physical storage of data and back-up copies within the national territory"* - author's note] *within the national territory*".

It would appear that as a result, Italy will have to similarly reformulate art. 9, para. 2 DPCM within the maximum allowed term of **30 May 2021**: indeed, this date seems only partially compatible with the expiry of the aforementioned DPCM, once the new AgID guidelines on the formation, management and storage of electronic documents comes into full effect (which should be 9 June 2021, considering the approval procedure and timing demanded by application of art. 71 of the Digital Administration Code) as established by art. 65, paragraph 10 of Legislative Decree no. 217 dated 13/12/2017, amending the DAC itself.

23 This was announced on the AgID website on 1 April 2020 https://www.AgID.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/04/01/precisazioni-sulla-pubblicazione-nuove-linee-guida-sulla-formazione-gestione

24 "*Without prejudice to the provisions of the Cultural Heritage Code, for the supervision thereof by the Digital Italy Agency the data storage systems of the Public Administration and those of other accredited entities shall envisage the physical storage of data and back-up copies within the national territory and assure access to data at the establishment of the controller thereof and security measures in compliance with those established by these guidelines*".

As for the other provision, namely the amended 33-*septies*, para. 1 L.D. no. 179, 18 October 2012, on one hand, this provision contemplates alternatives which limit its binding nature, and as previously noted, on the other could be traceable to one of the exceptions contemplated by the European legislation in question, for example to internalization (internal organization, see below).

Free circulation - Public security exceptions and internal processing

It is worth pausing on two limits to the application of the European discipline: the first with effect on the internal organization of the member States, the second on public security requirements.

As to the first, the last sub-paragraph of art. 2, para. 1 states: "*This Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organization of Member States and that allocate, among public authorities and bodies governed by public law defined in point (4) of Article 2 (1) of Directive 2014 / 24 / E.U., powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as the laws, regulations, and administrative provisions of Member States that provide for the implementation of those powers and responsibilities.*". The sense of the provision is better clarified by Recital 14, which reads as follows: "*As in the case of Directive 2014/24/EU, this Regulation is without prejudice to laws, regulations, and administrative provisions which relate to the internal organization of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as the laws, regulations and administrative provisions of Member States that provide for the implementation of those powers and responsibilities. While public authorities and bodies governed by public law are encouraged to consider the economic and other benefits of outsourcing to external service providers, they might have legitimate reasons to*

choose self-provisioning of services or insourcing. Consequently, nothing in this Regulation obliges Member States to contract out or externalize the provision of services that they wish to provide themselves or to organize by means other than public contracts.". As indicated in the quoted *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, "*typical examples include the use of a government cloud or a government engaging a centralized I.T. agency to provide data processing services for public institutions and bodies*"[25], a hypothesis that seems to fall within the sphere of the aforementioned art. 33-*septies*, para. 1, at least until private subjects with contractual remuneration become involved.

As to the second limit, consisting of processing for **public security** reasons in compliance with art. 4 of the Treaty on European Union (TEU), note that the concept of "public security" must be adequately defined and delimited, not in a loose or generic manner but in accordance with article 52 of the Treaty on the Functioning of the European Union (TFEU) and 5 of the TEU. It must be interpreted within strict margins, just as all exceptional norms limiting rights of a general nature (EU Charter 52, para. 1). It is useful to note that Recital 19 of (E.U.) reg, 2018/1807 gives a legal definition of "public security" updated to the relevant case-law of the E.U. Court of Justice, which we feel appropriate to quote: "*The concept of 'public security', within the meaning of Article 52 TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. It presupposes* ***the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society,*** *such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests. In compliance with the* ***principle of proportionality****, data localization requirements that are justified on the*

25 Ibid. pages 17-18.

grounds of public security should be suitable for attaining the objective pursued, and ***should not go beyond what is necessary to attain that objective***".

On the other hand, in the General Data Protection Regulation (GDPR) similar observations with respect to localization requirements cannot be found, given that the principle of the free circulation of data is not only acknowledged but explicitly constitutes a founding pillar of the regulation, naturally alongside that of the construction of a solid core of guarantees protecting data referring to natural persons. The two conceptual poles - free circulation and individual protection - need to dialogue. On closer inspection, the very extraterritorial scope of art. 3 GDPR on one hand and, on the other, the guarantees contemplated for data transfers to third Countries (Chapter V) lend themselves to interpretation in relation to the underlying principle of freedom of circulation (see Recital 6 GDPR: "*Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations while ensuring a high level of the protection of personal data*"). Putting the relationship between the two bodies of law in these terms, we could effectively ask what reasons could justify, even in the absence of explicit prohibition, the lawfulness of localization obligations with respect to personal data processing, given that the personal nature of the data appears only linked with the need for adequate protection and not the physical localization of the *data centres* in a specific Member State, and also considering the fact that the GDPR assumes the level of guarantee *ex lege* as identical in each member State[26].

26 It may be of some use to include an extract from the observations of Roberto Viola, director general of DG Connect at the European Commission, given the imminent introduction of (EU) reg. 2018/1807, see Id., *Free flow of data in the EU – a pathway into the cloud*, 12 November 2018, https://ec.europa.eu/digital-single-market/en/blogposts/free-flow-data-eu-pathway-cloud: "*Thanks to the new General Data Protection Regulation (GDPR), rules on the free movement of personal data in the European Union have been clarified and citizens' data is now guaranteed to be protected. Until recently however, there was no legislation dealing with the free flow of non-personal data in European legislation. At the same time, several Member States introduced legislation requiring certain data to be stored or processed within their national borders. These " " 'data localization requirements' " " were hindering the development of the EU data economy by stopping the emergence of data innovation ecosystems across European borders. They were also creating inefficiencies by requiring companies active in multiple Member States to duplicate IT infrastructure*".

Even regardless of the above, practical difficulties are certain to arise in distinguishing between systems that process personal data and non-personal data, considering that, on one hand, systems can easily be mixed and, on the other, that the concept of "personal" data is pervasive and dynamic: to put this more clearly, if a non-personal dataset can be associated at a certain point with a personal dataset, and vice-versa if a personal dataset can at a certain point be deprived of the component associating it, even indirectly, with a natural person, it becomes a non-personal data set. Against this mobility of qualification, localization does not appear sufficiently flexible to permit its adoption.

The existence of mixed personal and non-personal datasets is, in effect, considered by the legislator in art. 2 para. 2 of (E.U.) reg. 2018/1807, according to the criterion summarized in *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, p. 9[27]:

- *the Free Flow of Non-Personal Data Regulation applies to the non-personal data part of the dataset;*
- *the General Data Protection Regulation's free flow provision 26 applies to the personal data part of the dataset; and*
- *if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the General Data Protection Regulation fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset*.

It is evident that despite these indications, the level of complexity postulated by the existence of mixed processing poses questions that require careful examination such as, for example, the notion of "*inextricably linked*". Moreover, the approach indicated does not take into account the "osculant" nature of personal data previously alluded to.

27 COM (2019) 250 final, 29 May 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN

Dual standards and substantial approach

Earlier in the paper, we dealt with two questions, now the subject of intense debate, associated with the extraterritorial scope of part of the public legislation of third Countries. In order for these to be duly appreciated in all of their legal implications, we should contextualize them through a change in perspective. It would seem right to move from one of the fundamental considerations of the Schrems II ruling, expressed at various points of the motivation and summarised in § 180, where, in reference to the broader considerations developed in §§ 175 and 176, we find the following maxim: "*a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards*". That is to say, the reference is to a substantial approach to the observance of the rights of the person, which is necessarily lateral: it cannot, therefore, be limited solely to flows of personal data toward third Countries. In other words: the standard of the guarantee of the rights of the person applied against third Countries must be applied with equal rigour within the European Union. So, we wish to draw attention to the fact that one of the principal matters of debate, namely, interference for surveillance purposes connected with *intelligence* activities, meets a legal limitation within the Union in art. 2, para. 2 of the GDPR[28]. This evidently constitutes a paradox of which we must be aware: what is not "let past" by exception outside the E.U., is admissible within it. If the *rationale* of the entire discipline is, in the final analysis, the protection of the fundamental rights of the natural person, we cannot but notice that part of the very reasons for dissatisfaction legitimately expressed with respect to processing for the *intelligence* of third Countries, should also be valid for *intelligence* processing conducted intra-EU, however in this case the GDPR contains no provision for their activation.

28 In the end the quoted provision is inevitable since it forms part of the very architecture of the TEU and cannot disregard observance of Title V, Chapter 2.

Putting the question in these terms, a dual standard emerges ("two weights and two measures"), to which we would like to draw attention to in our overall legal assessment, and which is only mitigated by the idea that it could, in part, be compensated by art. 8 of the European Convention on Human Rights, a provision that identifies no a priori exclusions but rather a balance between the protected interests, which as such presuppose reasoning on merit.

Moreover, even if we depart from the considerations expressed with regard to the material scope of application of the Regulation, in the Union, there are still situations of interference by the public authorities, of unjustified limitation of the rights of data subjects or even the suspension of rights, which deserve to be considered with equal attention. In other words, the worry about what happens in processing conducted by the authorities of third Countries is right and justifiable but is recognizably affected, in actual terms, by a manifest form of juridical strabismus. To quote the most visible form: the introduction of generally extended and penetrating limitations in the application of the Regulation imposed by the Hungarian government with decree n. 179, 4 May 2020 raises equally serious perplexities with respect to the *intelligence* activities of non-EU authorities, because it takes place precisely within the Union, and because it regards the concrete applicability of the entire Regulation. Not surprisingly, the European Data Protection Board (EDPB) already took a stance on the matter at its thirtieth plenary session[29].

Even apart from the extraordinary case mentioned above, within the Italian legislation itself, there are ample reasons for perplexity regarding the compatibility of various limitations imposed by the fundamental rights of data subjects in their interactions with the authorities. Solely by way of example, we can cite the existence, however incredible, of a generalized and *erga omnes* requirement to store telephone and telematic data to contrast terrorism, international or otherwise, introduced by art. 24 of Law no. 167, 20 November 2017, a law

29 See EDPB, *Thirtieth Plenary session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR*, in https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en

that leads us to make an interesting comparison with *Section* 702 of the FISA; however, the latter at least envisages procedural guarantees and offers protection to the citizens of the Country that introduced it. Seneca is attributed with the phrase "*Aliena vitia in oculis habemus, a tergo nostra sunt*", the vices of others we have before our eyes, our own are behind our backs.

As a further example for the case of Italy, we can also cite the vast prerogatives existing in parliament for reasons associated with *autodichia* (the exercise of judicial powers by an administrative body), which also regard the legal area protected by the GDPR or the formulation of art. 2-*duodecies*, L. Dec. 196/03 (Italian Privacy Code), which like 2-*undecies*, evokes substantial confusion as to its compatibility with art. 23 of the GDPR. Likewise, the full coherence of the institute of preventive wire-tapping established by art. 226 of the implementation provisions of the Italian code of criminal procedure with the structure of the European unitary guarantees needs to be verified with a view to bolstering the protective measures if deemed necessary after such verification.

Let it be clear, the critical issues in national law and the structural issues of Euro-unitary law (e.g. art, 2, para. 2 GDPR) are of no use in rectifying data processing not sufficiently protective of fundamental rights conducted by third Countries; however, such European and domestic criticality requires a realistic interpretation and an honest acknowledgement: paradoxically, to actually avoid the application of an unjustified dual standard, we cannot exclude the possibility of suspending, with immediate effect, processing activities even within the Union, with consequences that would be paralyzing, and therefore impracticable.

It would be better, in the end, to contextualize the Schrems II ruling in the broader context of matters that also concern the domestic and European situation, and draw realistic conclusions with regard to the need to chart a direct course for achieving a general level of protection compatible with the legal guarantees.

Conclusions

The national cloud project in the Italian case and the parallel Gaia-X project under Franco-German guidance outline a scenario from which emerge clear indications of legislative policy directed toward the creation of cloud infrastructures under the full, or predominant control of member States and, but for now only a future prospect, of the European Union. Hence we consider this as the mainstay of our argument. It should be noted that the domestic and European motivations underlying the initiatives discussed seem, even in the light of the declarations accompanying them, to lead back more to strategic and political interests in bolstering digital sovereignty, than to authentic worries about the level of protection of fundamental rights within the Union.

In this sense, namely that of the effective level of legal protection, we should note that problems raised in the so-called "Schrems II" ruling of the Court of Justice of the European Union – a ruling we can either criticize or agree with but certainly not disregard – do not seem to be entirely eliminable through the mere intra-EU localization of the infrastructures, because these are substantially connected with the extraterritorial scope of the public legislation of third Countries. We could start international negotiations with these Countries, experimenting forms of *soft suasion*, but these would inevitably encounter limits in the national sovereignty decisions of those countries. So, realistically is seems improbable we can avoid the alternative black-or-white choice of whether to completely interrupt extra-EU flows of personal data, including those essential and inalienable connected with the very availability of cloud infrastructures today (acknowledging the enormous consequences this would lead to) and enable the exercise of fundamental rights and freedoms – this being a path in clear contrast with the principle of proportionality pursuant to art. 5 of the Treaty on European Union; or whether to concentrate attention on more balanced and proportional transitional models, aimed at creating infrastructures less dependent on foreign providers, but nevertheless 'ecosystemic' with said providers, ensuring adequate timing and design.

In this phase of transition, it would be reasonable to turn to pragmatic solutions and rely on providers with structure and capital able to offer guarantees of legal resilience in the event of prejudice, and assume the obligations required by the applicable European legislation, first and foremost the GDPR.

Among these pragmatic solutions, the following three are worthy of mention: the segregation of information considered strategic, the application of encryption methods directly usable by clients/users, and the study of juridical models for the management of the European infrastructures which ensure greater European control, while not forgoing the technological contribution offered by the extra-EU providers chosen from the market.

In the overall assessment of protection and with a view to a correct and overall balancing of risk factors, alongside the so-called "extraterritorial" risk described above, we should not neglect other aspects of risk, namely the risk typically presented by cybersecurity breaches, the impact of which on the fundamental rights of data subjects is particularly intense and pervasive (also because it includes the area of government attacks traceable to third Countries conducted outside the framework of the public security legislation of the attacking countries). From this point of view, the choice of cloud provider must be made taking account of the effective quality level that can be offered in terms of the State of the art and technology, that is to say, giving due consideration to the precedent given by responses to critical situations, the investments made in terms of continual technological updating, the eventual insurance coverage that can be provided in case of compensation, the SLAs (*Service Level Agreements*) and PLAs (*Privacy Level Agreements*), the quality and frequency of internal and external audits even with respect to organizational measures and the effective levels of training given to the authorized data processors, not only with respect to knowledge of I.T. (including countering *social engineering* techniques, but also with respect to awareness of the legislation.

Authors

*__Luca Bolognini__ (l.bolognini@istitutoprivacy.eu) is President of the Italian Institute for Privacy. European data lawyer, he is founding partner of ICTLC - ICT Legal Consulting law firm, with offices in Rome, Milan, Bologna, Amsterdam, Madrid, Helsinki and Melbourne, and serves as an Ethics & Privacy Advisor for several EU Horizon 2020 research projects. During the last 10 years he published juridical essays with RCS Etas and Springer, and co-authored with Enrico Pelino three volumes published by Giuffrè Francis Lefebvre – among which "Il Regolamento Privacy europeo", the first Italian commentary to the GDPR (2016) and "Codice della Disciplina Privacy" (2019), a complete commentary to the GDPR and all the Italian data protection and privacy laws. Luca also authored the pamphlets "Generazione Selfie" (Corriere della Sera, 2014) and "A.I. - Artificial Insanity" (Rubbettino, 2018).

**__Enrico Pelino__ (avv.enricopelino@griecopelino.com) holds a PhD in IT law from the University of Bologna and is a lawyer with an expertise in data protection and privacy. A frequent contributor of many IT and legal reviews, he co-authored with Luca Bolognini three books on the GDPR and the Italian data protection Code with Giuffrè Francis Lefebvre. Enrico is a speaker in conferences and mastercourses, he is also a Fellow of the Italian Institute for Privacy.

www.istitutoitalianoprivacy.it