FONDAZIONE NAZIONALE GIUSEPPE CAPOGRASSI

RIVISTA INTERNAZIONALE DI FILOSOFIA DEL DIRITTO

2

Anno di fondazione 1921
Serie V - aprile/giugno 2024

EU data institutionalism

scritti di
CATANZARITI, RUGGIU, MARONI, FIA, BROZZETTI

DE NARDO, *Democrazia sociale costituzionale*
DIMITRI, *Schmitt e il "nemico" oggi*
PISACANE, *Sulla "Città degli esclusi"*
BOUKEMA, *On western hubris*

GIUFFRÈ FRANCIS LEFEBVRE

Spedizione in a.p. - 45% - art. 2 comma 20/b - legge 662/96 - Filiale di Varese - ISSN 1593-7135

SOMMARIO

EU DATA INSTITUTIONALISM

Filiberto E. Brozzetti, Mariavittoria Catanzariti, *The Lexikon of Digital Institutions and the Remit of EU Data Institutionalism* 235

Mariavittoria Catanzariti, *EU Data Institutionalism: A New Compass for an Old Circle?* 239

Daniele Ruggiu, *Institutional Gaps of the Protection of the European Citizens' Personal Data: For a "Rights-Based Digital Sovereignty"* 263

Marta Maroni, *The Idea of Data and European Constitutional Imaginaries: An Immanent Critique of the Data Governance Act* 285

Tommaso Fia, *Unfair Terms Review in the Data Act: An Effective Means for Institutionalising Data (Markets)?* 317

Filiberto E. Brozzetti, *EU Digital Sovereignty: How Long Will the "Brussels Effect" Last?* 343

STUDI

Valentino De Nardo, *La democrazia sociale costituzionale. Fra la democrazia liberale e la democrazia socialista* 379

Nicola Dimitri, Distinguo ergo sum. *Per un uso critico della categoria del "nemico" di Schmitt nella temperie odierna* 399

Salvatore Maria Pisacane, *Dal diario di un viaggio nella "Città degli esclusi": uno sguardo critico sugli attuali modelli di convivenza sociale* 435

Henk-Jan M. Boukema, *The Remains of Western Hubris* 449

Institutional Gaps of the Protection of the European Citizens' Personal Data: For a "Rights-Based Digital Sovereignty"*

Daniele Ruggiu

summary: 1. *Introduction*; 2. *The Role of the General Data Protection Regulation in the Globalised Circulation of Data*; 3. *The Global Circulation of Data and the Extraterritorial Application of the GDPR*; 4. *The Chinese Example. What about Europe?*; 5. *Conclusions*.

1. *Introduction*

Today the functioning of our economies is based on the circulation of data and this circulation is global. The data represents not only the new petrol of the market, but also the real engine that moves the modern economy. No sector is spared by the digital revolution: the labour market with digital platforms, automated forms of recruitment, the control of the performance of work tasks, the industry with automated forms of production, research with the transversal use of the digital technologies, the administration, the justice administration, the military, all the sectors base their functioning on the circulation of data. The importance of data is such as that digital technologies not only produce data, but they are produced with this main purpose. Thus, contrary to what we think, today the main business of the big Silicon Valley companies is not the develop-

(*) PRIN 2022KTTSBC – CUP Master D53D23007300006. "Digital Sovereignty in Comparative Perspective: State Authority, Corporate Power and Fundamental Rights in Cyberspace" University of Salerno | University of Padua.

ment and production of services and products although digital, but the data processing[1]. Today technologies are sold not for supplying products and services but for producing data. In this sense, the infrastructures that allow the global circulation of data are crucial.

The global dimension of internet and the flow of data that circulate worldwide raise several problems, however, due to the intersections of different jurisdictions inspired to different principles and values that hardly can be coordinated and easily clash. In particular, it is pretty complicated applying the principle of territorial jurisdiction to objects like the cloud-stored data that cross countries at the worldwide level and characterised the current era of internet. Where is data? Everywhere. Nowadays internet increasingly refers to the cloud as a tool for storing the data that stem from everywhere. The cloud is the infrastructure that ensures the global circulation of data to both businesses that exploit them and consumers that need to rely on the endless services of internet. This has several advantages, economic, storing, accessibility, usability etc. but opens to potential conflicts of jurisdictions among countries.

In this context a protectionist legislation in the field of the circulation of data can represent an obstacle for the innovation and the economic and financial development not only of single countries, since it can affect the global market. In this regard, given the exceptional nature of data, completely different from any other good regulated by the law, some claimed for a broad political agreement at the international level that defends the good of the free access to data from everywhere (bypassing thus any legislation on privacy)[2].

In Europe the regulation of the digital data falls under the General Data Protection Regulation (GDPR) that up to now proved to keep the pace with the technological progress even in the age of cloud computing.

The GDPR represents an exceptional case of regulation in a continental market that is entirely inspired to the implementation

---

([1]) S. Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, in «New Labour Forum», 28, 1, 2019, available at: https://www.oru.se/contentassets/981966a3fa6346a8a06b0175b544e494/zuboff-2019.pdf

([2]) https://www.bloomberg.com/news/newsletters/2022-02-10/is-facebook-going-to-have-to-pull-out-of-europe.

of a principle: the principle of "privacy by design", namely a right. This regulation is thus based for the first time on a right (the right to data protection to be precise) and it has imposed a rights-based model of governance[3] at the worldwide level being able to drive the crucial sector of the digital market at the global level. A case that didn't stop the innovation in Europe and in the world. Its extraterritorial application raises though problems and risks compromising its effectiveness, renewing the question of the regulation of data that are destined to circulate globally.

At the world level there are examples like China and Russia that opted for solutions different from extraterritoriality, enforcing their digital sovereignty with the provision of the "data localisation", namely the obligation of localising the data servers that handle data of citizens within the country. In particular, the case of China appears interesting with regard to a possible strengthening of the protection of the privacy of the European citizens since it combines the means of digital sovereignty with the goal of the protection of rights.

This article is articulated as follows. First, I will describe the importance of the GDPR compared to any other legislation on privacy. Then, I will briefly explore the debate between data exceptionalism and data institutionalism in front of the increasing trend of the internet market of being based on the cloud computing. Third, I will cope with the topic of the rise of the Chinese regulation on privacy shifting between the U.S. model and the European one and I will focus on the introduction of the data localisation, a measure that has not messed up the markets that increasingly rely on global platforms and cloud storing infrastructures. Finally, I will conclude that this solution is functional to the protection of values that are central in a given legal order and since these values coincide with fundamental rights, given the strict link between privacy a civil and political liberties, data localisation should be considered not only for the protection of the EU market and privacy in Europe but as a shield for the liberties of the European citizens.

([3]) D. Ruggiu, *Human Rights and Emerging Technologies. Analysis and Perspectives in Europe*, R. Brownsword's preface, Pan Stanford, Singapore 2018, p. 208

2. *The Role of the General Data Protection Regulation in the globalised circulation of Data*

The General Data Protection Regulation (2016/679) represents an *unicum* at the worldwide level establishing not only the highest level of protection of privacy compared to that provided by any other country, but also a model of innovation that can be deemed as an alternative to that one that is based on an almost unlimited employment of data as its core business. Although the market centered on data and leaded by high-tech companies, largely informs all the current economies, making the technologies that are needed for collecting, storing and processing data the main ingredient of the neocapitalist recipe of the 21st century, this renewed attention for the importance for data protection has led to an alternative form of business that has showed to be pretty competitive. Not only there are increasingly more services, apps, job positions for the protection of privacy (e.g. Data Protection Officer), but there are some companies that use privacy and data protection as a label, pretty effective, for succeeding in the market. The fact that these companies are far from being little means that a different form of innovation is possible even in a field, the digital one, that could not exist without data. No computer, app, platform can be conceivable without data. Our present is digital, namely largely based on the processing of data.

This also means that the GDPR is a competitive regulation, and rules and the protection of rights as such do not hinder innovation but only address a different form of development.

If we consider the fact that the GDPR regulates a field that crosses transversally all the digital technologies that, in fact, need data for functioning, and that the data that they produce are central in modern economies, we can conclude that GDPR plays a central role in the economies, not only European. As noted by Shoshana Zuboff[4], the data represents not only the new petrol of the market, but also the real engine that moves the modern economy. The importance of data is such as that digital technologies not only produce data, but they are produced with this main purpose. Contrary to what we perceive,

---

([4]) S. Zuboff, *Surveillance Capitalism*, cit.

the main business of the largest IT companies is not the development and production of digital services and products, but the processing of data that can be used for predicting the behaviour of people that with this new value can be sold again and again. Digital technologies have become the trojan horse for the circulation of data. Our data. This means that if we buy a phone, a computer, earphones, a smart tv, Amazon Echo or a subscription to Amazon prime, or Netflix, what is sold is not a good or a service, but our data that will be in turn sold to third parties. Today, this represents the major asset of the companies engaged in the digital. For example, in 2001 Google's revenue shifted from 86 million US dollars in 2001, to 3,2 billion US dollars in 2004[5]. As noted, in postmodern economies we are the product and the forecast about our future behaviour (profiles) is the new value for this market because advertisers and their clients are interested in guessing what we could need[6]. But also other parties can be interested in this information, like politicians, for example, law enforcement bodies, foreign countries etc.

And since profiles can always be better and more precise, the need of new data, of new programs and algorithms for processing them is almost endless.

This makes the circulation of data the real value, the good for which it would be worth to make a war. Like the water in a drought era.

In this context a regulation able to cover a whole continent is of paramount importance, especially if we consider the fact that the GDPR is completely centred in the protection of an individual right: privacy. All the provisions of the GDPR are devised for the protection of the right to data protection, and the implementation of the principle of "privacy by design" that mainly apply to the development and programming stage of the digital technologies. This particular rights-based architecture and its central role in the governance of the digital sector due to the centrality of data, makes the GDPR a rights-based tool of governance that is not only able to influence the digital market in Europe, but, considering the extent of the European market, as well as its interrelations with all the other markets, to affect the whole

---

([5]) Therein, p. 14, https://www.oru.se/contentassets/981966a3fa6346a8a06b0175b544e494/zuboff-2019.pdf.

([6]) *Ibidem.*

digital market in the world, since almost any company that produces and sells digital services and products has to sell those same services and products in Europe. This coincidence of the extension of its market, Europe, and the importance of data for almost any technology has transformed the EU, that is a "political dwarf" (fragmented in a collection of 27 sovereignties), in a "regulatory giant" in the world[7]. An example that has been replicated with the AI Act with regard to the artificial intelligence. Thus, we should not be surprised for the fact that the GDPR succeeded influencing the whole disciplines of cookies at the European level and there were several resounding cases of application of the GDPR provisions: the case of the stop of ChatGPT by the Italian Data Protection Authority (20 March 2023)[8], for example, or the case of the fine of 1,2 billion for Meta by the European Data Protection Board for the illegal transfer of the data of EU citizens to US (22 May 2023)[9]. But considering the scope of this market, and its enormous value, we should not be surprised that many, like Mark Zuckerberg, repeatedly quested for the overcoming of this successful regulation via politics. Despite this success, however, we could be more surprised that some European institutions proposed some regulations that go in the opposite direction of the GDPR. First, with the Directive on the Secondary use the EU juxtaposed the opposite principle of "open data by design" to that of the "privacy by design" that was enshrined in GDPR[10]. Second, with the proposal of the Chat control 2.0 regulation the EU would like to overcome the end-to-end cryptography that defends our chat and email communications in the name of the fight against child pornography. In the first case, any private can have access to the data stored by the public sector by default. In the second case, the chat and email providers are obliged to save a copy of the content of all our communications that today are invisible to third parties creating a permanent accessibility

---

([7]) D. Ruggiu, *Spazio economico, tecnologie digitali e decostruzione dello spazio normativo del soggetto*, in «Ars intepretandi», 2, 2024, p. 75.

([8]) See https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/ 9870847 #english.

([9]) See https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

([10]) See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L 1024.

of the data that we generate. Not only, to private businesses but also to the law enforcement agencies.

Probably the lesson learnt with Cambridge Analytica[11] and the Edward Snowden[12] case has been forgotten.

3. *The global circulation of data and the extraterritorial application of the GDPR*

The importance of the GDPR is also underlined by its extraterritorial scope that makes its provisions almost a shield that follows European citizens even outside the Europe. This is a demonstration of power of this regulation and its wish of protection the rights of citizens wherever they are, but it is also a source of problems, theoretical, political and legal.

Nowadays, the GDPR's extraterritorial application risks to create several problematic instances of conflicts of jurisdiction in the age where all data are global and the cloud is the measure of this general trend. As known, the GDPR claims protection of all data subjects that reside in the EU, regardless of their nationalities, and regulates cross-border data transfers towards non-EU countries, thus being applicable to the controllers and processors that are not on EU territory, but process personal data of natural persons in EU. The aim was clearly of strengthening the protection of data at the European level and putting a stop to those who wanted to elude the EU standards[13]. However, the achievement of this purpose in a widely globalised market is not easy at all. In fact, in the age of the cloud, where all da-

---

([11]) In 2014 Cambridge Analytica, a society made for using strategic communication strategies in the political field, used a personality test on Facebook for profiling the Facebook users that downloaded it (around 270.000) and then all their Facebook contacts creating 87 million of profiles worldwide that have been used for making a targeted communication and influencing the Brexit referendum first and then the 2016 US election that led to the Donald Trump's presidency.

([12]) In 2018 an ex-CIA Agent, Edward Snowden, revealed that following the 9/11 terrorists attack in 2001, the US National Security Agency created a gigantic system of mass surveillance of the American and non-American citizens within the US and abroad owing to the help of the main US private internet and telecom providers and the cooperation of the foreign secret services of the US allies (British, Canadian, Italian tec.).

([13]) See the GDPR's whereas nn. 113 and 116.

ta are archived in the cloud this can be the source of endless conflicts and can lead the GDPR to a lethal ineffectiveness[14].

In the data-centric turn of the market, the wide circulation of data is crucial, since this model of business needs infrastructures that are able of overcoming the physical and legal limits of the informative circulation. Whilst in the past data and software were used to being stored on a local machine – such as a cell phone or computer – today that data is stored remotely on faraway servers, which can be accessed by a network such as the internet. This is the advantage of the use of the cloud computing[15]. According to the estimates, in 2019 the 55% of the consumer Internet population used personal cloud storage, and 86% percent of data processing will happen remotely in cloud data centers, rather than locally[16]. The cloud computing is the supply of informatic resources (like archiving, power of processing, databases, net, analysis, AI, software applications) on internet (the cloud). This allows to reduce the costs, to increase the power of processing and the amount of data processed, to archive the data on a physical hardware that is distributed at the global level and to shop the rules that could be applicable to the data largely eluding the application of the provision of a regulatory system. Like GDPR. Cloud computing is the perfect infrastructure for Big Data that flow across internet. With the cloud, the internet has become globalised and personal data have been subject to a process of "internationalisation". However, this phenomenon is only apparently delocalised. Whilst the internet users are located outside the United States, the largest glob-

---

([14]) Z. Bo, *Data Protection as Fundamental Right: The European General Data Protection Regulation and its Extraterritorial Application in China*, in «US-China Law Review», 16, 3, 2019, p. 99.

([15]) For example, e-mail has largely shifted from being a local service to being a cloud-based service. In the past, if a user sent an e-mail, she retained a copy on her machine and the recipient retained a copy on her machine. So, both users saved a copy of the email in their inbox and each user was responsible for storing and maintaining the inbox, much like physical mail. The inbox is now managed by a third party that stores the e-mails on its own servers rather than on the user's computer, and users access these remotely stored inboxes whenever they need them, using a series of different tools – websites, applications, and so on. The same shift occurred for any other digital goods liker, photos, music, movies, on line banking etc. Cfr. A. K. Woods, *Against Data Exceptionalism*, in «Stanford Law Review», 68, 2016, p. 740.

([16]) Therein, p. 741.

al technology companies are currently U.S.-based[17]. Expanding into foreign markets is a top priority of the internet companies.

The union of cloud computing and globalisation has led to a separation of the individual from their own data that are stored in far distant centres and subjected to several jurisdictions.

Considered that while the European citizens circulate outside the European borders their data could fall under different regulations with different levels of standards and that the data controller could transfer the data to third parties that are located in other countries with a lower level of protection, the GDPR's answer was its extraterritorial application but this has created a several problems of application. In particular, the principal infrastructure of the globalised era, the cloud, severely endangers the application of the GDPR provisions. In this context the extraterritorial application risks to become a boomerang, transforming a potential success in its opposite, leading the GDPR to the ineffectiveness rather than to its extraterritorial implementation.

In fact, the architecture itself of the circulation of data at the global level, the cloud, risks to be the window through which our data flow and escape in the hands that are outside the EU. Although the data travel on a cloud the databases where data are archived and processed are on the ground, in a well identified location[18]. Differently from what we think data need physical supports and the location of the storage hardware determines the jurisdiction and the applicability of the rules. Thus, the circulation of data seems to be subjected to two different and opposite forces: one that tends to impose rules that are devised for implementing the principle of the "privacy by design", one that tends to elude these same rules. The circulation of data seems subjected to two schizophrenic forces: GDPR and the market.

Moreover, cross-border data transfers can happen in unexpected ways, bringing up greater data protection concerns at global level[19]. For example, Facebook has data sharing partnerships with at least four Chinese electronic companies dated back to 2010, offering broad private access to user data to Huawei, Lenovo, Oppo, and TCL

([17]) Therein, p. 742.

([18]) The biggest database in Europe is Supernap and it is located in the nearby of Pavia. See https://timelapselab.it/it/notizie/supernap-data-center-siziano.html.

([19]) Z. Bo, *Data Protection as Fundamental Right*, cit., p. 98.

without user's consent. Such data sharing allows the Chinese partners to retrieve detailed information on both device users and all of their friends, including religious and political leanings, work and education history, and relationship status[20]. Similar data sharing agreements were made by Amazon, Apple, BlackBerry, and Samsung[21].

The extraterritorial application seems thus really problematic.

3.1. *Data Exceptionalism versus Data Institutionalism*

This dualism between the two opposite tendencies related to our data has led to an interesting debate between those that support the globalised trend of the market based on technological infrastructures like the cloud[22] and those who defend not only the need of regulating the flow of data, but also hold that this is possible, as we always regulated any other good[23]. The focus of the debate is thus if data are a good like any other else (or they are an exception that need its own rules) and which institutions are needed in the regulation of data.

According to the advocates of the "data exceptionalism", modern technological life needs global cloud for storing and processing billions of data stemming from anywhere. It is the sign of time. And the cloud is the infrastructure that allows this huge integration of data that is needed by the quest of new and more efficient services that meet the continuous creation of apps, digital platforms, archives and the exchange of increasing amounts of data. This, however, tends to escape the traditional jurisdictions and it should thus request new apposite international regulations, that up to now do not exist yet, and that need a wide international agreement where the main geopolitical powers, USA, Europe, China, agree on how to regulate the global

---

([20]) *Ibidem*.

([21]) M. LaForgia, G. J. X. Dance, *Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence*, in «The New York Times», 2018, available at: https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html; S. Liao, *Why Facebook's Secret Data-Sharing Deal with Huawei Has the US Concerned*, in «The Verge», 2018, available at: https://www.theverge.com/2018/6/8/17435764/facebook-data-sharing-huawei-cybersecurity.

([22]) Z. D. Clopton, *Data Institutionalism. A Replay to Andrew*, in «Woods Sanford Law Review», 69, 7, 2016, pp. 9-16.

([23]) A. K. Woods, *Against Data Exceptionalism*, cit., pp. 729-789.

market of data. This is a mere technical problem that must find a political solution. Since the phenomenon is global this solution must be reached at global level. The problem can be summarised as follows: «while many people now store their most personal data in the cloud that is, on remote servers scattered around the globe — there is no settled understanding of who has jurisdiction over that data»[24]. Data escape traditional forms of regulation so it is almost useless to pretend to treat them like any other object. "[C]loud-stored data is fundamentally incompatible with existing territorial limits on jurisdiction" [25]. Simply this is not a legal question. It is political.

According to the advocates of the "data institutionalism", «the "cloud" is actually a network of storage drives bolted to a particular territory», and there are reasons, as well as substantial case law, for thinking that data are a physical object that can be regulated like the old objects that we experimented[26].

On the background there is the important question of whether we can expect a right to data protection over those data that stem from us, from our daily use of a number of endless devices, apps, platforms etc. and are then stored on a cloud.

This problem became apparent in 2013 with the *Microsoft Corp.* case[27] regarding the reach of the State's jurisdiction over internet data[28]. On December 4, 2013, a search warrant for the contents and metadata associated with an e-mail account stored by Microsoft was issued by a magistrate judge in the Southern District of New York. Consequently, Microsoft produced the metadata of its servers in the US but as many other internet companies, Microsoft often stores its data in data centers located around the world for better managing the data loads and ensuring that the user's data is promptly available wherever the user accesses it. The problem was that much of the data of this particular customer was stored on its data center in Ireland.

([24]) Therein, p. 732.

([25]) Therein, p. 734.

([26]) Therein, p. 732.

([27]) See Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467-68 (S.D.N.Y. 2014) [hereinafter *Microsoft E-mail Search Warrant Case*], appeal docketed sub nom. Microsoft Corp. v. United States, no. 14-2985-cv (2d Cir. argued Sept. 9, 2015).

([28]) A. K. Woods, *Against Data Exceptionalism*, cit., pp. 731.

So, Microsoft refused to hand over that data holding that the Stored Communications Act that regulates this matter does not apply extra-territorially. Unconvinced by the Microsoft's argument, the judge just repeated its warrant. According to the company allowing the U.S. government to compel the data would encroach on foreign sovereignty. And consequently, the Ireland stated that it was interested in the matter. Those data had a clear territorial origin.

The global scope of the cloud and its increasing use generated several jurisdictional disagreements like this of Microsoft. What should we do when two nations assert jurisdiction over the same piece of data? Moreover, the high-tech companies will likely find a safe shelter behind these argumentations escaping any risk of litigation. Just imagine Meta and Mark Zuckerberg. Few weeks ago, following the fine of the European Data Protection Board to Meta, the ex-Ceo of Meta stated that the problem of use of data in Europe is not legal, it is not a question of application of the GDPR provisions, but it is political: the EU and the USA should find an international agreement over the transfer of data of the European citizens everywhere. The GDPR should be just inapplicable… at least to Meta. It would be a paradox, if the main regulation of data in the world is not applicable to the largest companies that found their business on data.

However, the argument that data constitute an exceptionality on the legal world and they just need a special regulation can be rejected from several standpoints. Cloud-stored data is not as volatile as it appears, it has physical and tangible features. First of all, it is stored in servers that have a precise location and fall under a given jurisdiction. From the legal standpoint, in a free-floating ether cloud data is not a complete novelty. Like intellectual property, debts, bank accounts which have been the subject of extraterritorial seizures going back many years, data is not so different from any other form of intangible asset[29]. For identifying the jurisdiction over the cloud-stored data it is necessary to determine the location of the data, the domicile of the data controller, the location of the crime, the citizenship of the victim, and/or the citizenship of the perpetrator. As noted, this has much to

---

([29]) Therein, p. 735.

do with territoriality[30]. However, as seen, the existence of different bases for jurisdiction also means that the same piece of data may be subject to a number of different jurisdictions at the same time. And this, yes, can give rise to conflicts of jurisdiction but we must not forget that the law is full of such disputes and States can easily find a solution to this. So, nothing new under the sun of the law! The best analogy to offshore data storage is transnational litigation regarding offshore bank where blocking statutes, which prevent citizens from complying with foreign law enforcement requests, greatly exacerbate conflicts of laws[31]. In this field, statutes can foster the harmonisation and reduced the conflicts. So, in the field of cloud-stored data reforming of State's privacy legislation that often operates like blocking statutes, can reduce the number of transnational conflicts.

4. *The Chinese Example. What about Europe?*

In this debate about the cloud-stored data, the example of China in the regulation of the cloud-stored data can be somehow useful.

The regulation of the matter of the data protection in China much differs from both Europe (the comprehensive approach to privacy) and U.S. (the minimalist approach). Initially, as it happens in the U.S., there were several sectorial regulations of this matter in China. China avoided to enact a comprehensive regulation of privacy like in Europe (the GDPR), whilst it created several specific regulations in different sectors such as healthcare, finance, postal services, consumers protection, communications, credit. Only recently it started to adopt one regulation on privacy but with a sensitive difference between the public and private sector that reflects the specificity of the Chinese context, dominated by the collective and communist values, an authoritarian, single-party form of government and the non-respect of fundamental rights. This exceptionality involves especially the data protection before the public powers where few or no limitations ex-

---

([30]) *Ibidem*.
([31]) Therein, p. 737.

ist[32]. Whilst strong limits exist for the private sector. In other words, in China data protection covers only the "consumers", but not the "citizens" in their relationship with the public powers[33]. No privacy exists in front of the government but a system of mass surveillance.

Laws and regulations related to the data protection in China have a relatively short history. Only in 2020, China has made efforts to establish an overall data protection system.

First, the Chinese 1982 Constitution does not have any specific provision on privacy and data protection. There is only a far reference to freedom and privacy of communications in art. 40.

With the approval of the Decision on Enhancing Information Protection in December 2012 by the Standing Committee of the National People's Congress there have been started the legal initiatives for the protection of personal data in China[34]. This document regulates processing of personal information in both the public and private sectors and supported the protection of electronic information that could lead to the identification of individuals and violate their privacy. In 2013 the National People Congress' Standing Committee updated the Consumer Data Protection Law making data protection a distinct right for consumer with its art. 4[35]. In the same year the Ministry of Industry and Information technology (MIIT) adopted Telecommunications and Internet Personal Data Protection Regulation adding new rules for the collection and use of personal user data, providing minimum requirements for data collection, notice and data breach notifications[36]. In 2016 the Standing Committee of the National People's Congress adopted the Cybersecurity Law (CSL) that centralises dispositions on personal information protection, and represents one of the most important milestones in the data protection legal land-

---

([32]) E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the US and the EU?*, in «Penn State Journal of Law & International Affairs», 8, 1, 2020, pp. 49-117.

([33]) Therein, p. 54.

([34]) It states that its explicit goal is to protect the lawful interests of citizens and to safeguard the national security and the social order that is a unique to China and not found in the Eu and U.S. laws. Cfr. E. Pernot-Leplay, *China's Approach on Data Privacy Law*, cit., p. 69.

([35]) Therein, p. 71.

([36]) Therein, p. 72.

scape[37]. Here personal data are defined similarly to the GDPR and the data protection principles are closer to global standards. According to the Cybersecurity Law, similarly to the GDPR, the network operators collecting and using personal data must obtain the prior consent of the data subject and must abide by the principles of legality, property and necessity[38]. Moreover, the network operators cannot collect personal information not related to the services they provide, violating the laws and agreements with the data subject (art. 41). Principles of specification, transparency, lawfulness, data minimisation and consent[39] are affirmed in analogy of the EU regulation[40]. After this, on May 28, 2020 the Civil Code of the People's Republic of China was adopted and it opened to the Chinese data protection system as a comprehensive regulation getting closer to the EU and aligning with the core international principles of data protection law, establishing additional safeguards for sensitive data, for processing of personal information, the specification of the purposes for the processing of personal data and data portability[41]. The Code accompanies thus a patchwork of several laws including, beyond the Cybersecurity Law, the National Standards for Information Security Technology – Personal Information Security Specification, approved in 2018, and its updated version in 2020, the Data Security Law of the People's Republic of China, which has been in effect since September 2021, and the Personal Information Protection Law of the People's Republic of China, which has been in effect since November 2021, constitute the most significant legal initiatives in the field of data protection in this country.

Like in the U.S., China does not have a single independent supervisory authority, and it follows a multi-agency supervisory model, with multiple entities responsible for enforcing data protection regulations in their respective sectors. Thus, this puzzle of laws in dif-

---

([37]) Therein, p. 73.

([38]) *Ibidem*.

([39]) The Cybersecurity law however, allows also the implicit consent, requiring the explicit consent only when it is explicitly mentioned. Therein, p. 84.

([40]) Therein, p. 77.

([41]) Therein, p. 54.

ferent sectors is accompanied by a multitude of government agencies that can be competent in the field of data.

Moreover, it has to be noted that also the matter of data protection is affected by the typical generality and vagueness of the Chinese laws needing a number of non-binding documents and guidelines that play though a central role in its implementation. This gives the government bodies the needed room for manoeuvring and interpreting flexibly the provisions in line with the goals of the executive, and enforcing the law[42].

Following the Cybersecurity Law, with the adoption of the Civil Code that recognises the right to privacy and safeguards the personal information, China further demonstrates its own inclination towards a comprehensive system of protection of personal data[43]. Like in Europe. With a peculiarity: in a regime where the State's control over citizens is capillary and increasingly supported by new technologies, this system of protection with a strong mechanism of sanctions is addressed only to private individuals.

In this peculiar context we must understand the regulation of the cloud-stored data by China.

As for the territorial jurisdiction, as we know, the GDPR has an extraterritorial scope, since it may apply to companies that are located outside the Union while they offer services to data subjects in the Union or they monitor their behaviour when it takes place within the territory of the EU. Moreover, it applies to EU citizens abroad. The U.S. has also an extraterritorial scope, for example in California[44]. China legislation on privacy, instead, is applicable to operations that happens within the country[45].

Prior to the Civil Code, the Cybersecurity Law, as a specific law, also addressed security considerations related to the processing of personal data and, in this regard, it marks a turning point in the China's data protection landscape. An important feature of this law is the regulation of requirements for "data localization"[46]. According to this

---

([42]) Therein, p. 74.
([43]) *Ibidem*.
([44]) Therein, p. 81.
([45]) *Ibidem*.
([46]) Therein, p. 103.

law, personal information and important data collected or generated by operators in China must be stored within the country. Whilst the U.S. approach is basically against the data localisation restrictions as trade barriers so it provides no special requirements for transferring personal data from U.S. to third countries, the EU approach, as known, is more restrictive requiring for cross-borders data transfers the respect of the level of protection set by the GDPR. But, so far, no data localisation requirement has been set out yet. The Chinese approach is in its turn, more even restrictive affecting the cyberspace sovereignty. Cyberspace sovereignty[47] is part of the geopolitical strategy of China and in this context data localisation play a strategic role[48]. According to this principle, furthermore, if a network operator intends to transfer this data outside of China, it must demonstrate the necessity of the data transfer and implement security assessments (CSL art. 1). This clearly subjects the whole data flow in China to the Chinese regulation. And to its principles.

Clearly the principle reflects a country that has serious democratic limits. The Chinese data localisation, that took into effects several months after the CSL, is aimed at protecting the individuals' privacy but also the China's economic development and reducing the exposure of the country to the foreign intelligence. An analogous rule only exists in Russia.

Eventually, notwithstanding some activities lobbying against, no foreign company questioned this choice. Nobody left China. Moreover, as seen, several foreign operators like Facebook showed no concern in sharing with Chinese enterprises and State's agencies the data collected abroad although related to foreign citizens like EU citizens. No concern was raised for localising data, nor for sharing more data than necessary if this is the prize that has to be paid for the access to that market. Probably, these companies have less problems in sharing data even with countries that do not have strong democratic tradi-

---

([47]) According to the cyberspace sovereignty, cyberspace is subordinated to the interests and values of a country within its borders. Following the Edward Snowden's case, to ensure its sovereignty a country can exert control over the architecture of internet, content and data flows (such as imports and exports of data), restricting foreign content, usually for security reasons. This represents a strong break with the multistakeholder approach of the internet governance. Therein, pp. 104-105.

([48]) Therein, p. 104.

tions, like in this case, than in applying the rules aimed at the protection of privacy implemented by countries that are a benchmark in the protection of privacy. The rules of the market that request the widest circulation of data seems to be valid intermittently, according to the benefits it can gain. However, this clearly shows that the data localisation is not impossible due to the global nature of the market, or the technical considerations related to the exceptionalism of the matter. If data protection strongly depends on the localisation of the information, the implementation of the data protection by the GDPR needs the construction of coherent infrastructures and institutions such as the localisation of data-servers in Europe. In other words, there can be a version of digital sovereignty explicitly aimed at the protection of rights as a strategic asset of a political community. That we could call a "rights-based digital sovereignty".

5. *Conclusions*

The debate over the regulation of cloud-stored data and the data transfer see two opposite tendencies facing: one that holds that data signs an exceptionality among the concepts of the legal world and for this reason it requires a specific regulation based on a political agreement to be met at the international level; and one that holds that in the age of the globalisation of internet data behaves like many other intangible objects and like them can be regulated. On these two fronts two different approaches to data protection, the American and the European, also face. In this context the atypical example of the rising regulation on privacy, with all its contradictions, limits due to the specific political situation of the country suggests that regulation needs also the necessary institutions, administrative and legal, for its implementation. In 2016 China has introduced the data localisation with the Cyberspace Security Law. This rule provides that each network that collects and processes data in China must store that data in China. This restriction that has few comparable examples in the world can help to understand that if we want to implement the EU specificity we must to consider specific institutions for the protection of data. The debate over the cloud-stored data is not only technical, but technical and political. If the State's jurisdiction in a given matter

depends on the localisation of its object, maybe we should not be afraid to talk of cyberspace sovereignty. In a time where the world conflictuality crosses the borders, where internet has been the space of worldwide scandals, like the Edward Snowden's case and Cambridge Analytica, that clearly showed the substantial link between political vulnerability of our fundamental rights and data protection, to talk of digital sovereignty is not a taboo. Digital sovereignty aims at affirming that cyberspace is subordinated to the interests and values of a country within its borders. These values in Europe coincide with our fundamental rights and data protection and GDPR plays in this field a crucial role of defence of our democratic liberties. Following the Edward Snowden's case, to ensure its sovereignty a country can exert control over the architecture of internet, content and data flows (such as imports and exports of data), restricting foreign content, usually for security reasons. This represents a strong break with the multistakeholder approach of the internet governance[49]. After Cambridge Analytica we learnt that the way of processing data through mass profiling and transferring this data to increasingly unknown third parties can vulnerate our political liberties and the whole democratic architecture of a country. This gate was used by political movements that where hostile to the European Union. Not only foreign countries[50]. Thus, if we want to regulate the flow of data regarding the European citizens we have to build the institutional premises of the application of the territorial jurisdiction: namely we must claim that data are stored within the European continent and implement those infrastructures that are needed for safeguarding the gate of our liberties. We must build a kind of "rights-based digital sovereignty", an infrastructural architecture that is in accordance with the value architecture of a country (or a political community like the EU). At least until the next Cambridge Analytica scandal.

([49]) Therein, pp. 104-105.

([50]) Starting from few hundred thousand of profiles on Facebook, a British company named Cambridge Analytica, funded by ultraconservative American movements guided by Stave Bannon and Richard Mercer, was able to profile more of (unaware) 87 million of people in the world and to use these for influencing the Brexit referendum, and breaking up the European Union, first, and, then, the 2016 presidential elections in the U.S.

Abstract

Europe has affirmed a model of data governance with higher standards for the protection of the rights of the European citizens that distinguishes its market at the worldwide level. At the same time, this model can cope with the biggest high-tech players without hindering the business based on data, that today has become the major asset in our economies. Owing to the creation of effective institutions in the data protection, this model has showed to be able to affirm also an alternative model of innovation and of business, able to influence and orient the Silicon Valley companies and impact the rising sharing economy. However, the globalisation of the data circulation has proved that at the institutional level there is also the need of strategic policies for the creation of European infrastructures for the management of data since this directly affects the application of regulations on data. For instance, China has paid a great attention on the location of servers and databases and on the construction of its data sovereignty despite an atypical model of protection of privacy that is strong with the private sector and almost inexistent with regard to the public sector. The European market instead is characterised by a weak sovereignty on its data in front of a data market that often tends to send the data abroad where the laws on data are weaker and standards are much lower. This has led to an increasing pressure towards the policies amending of the European legislation on data (e.g. the Directive on the secondary use, the Chat control 2.0 proposal etc.). The major challenge for the European Union now is thus to invest on its institutional assets, building the conditions for its data sovereignty without dismantling its regulation on data but creating a better integration between these.

L'Europa ha affermato un modello di governance dei dati, con standard più elevati per i diritti dei cittadini europei, che caratterizza il suo mercato a livello mondiale. Allo stesso tempo, questo modello è in grado di tenere testa ai più grandi attori del digitale senza ostacolare il nuovo modello di business basato sui dati, che oggi è diventato il principale asset delle nostre economie. Grazie alla creazione di istituzioni efficaci nella protezione dei dati, questo strumento ha dimostrato di poter affermare anche un modello alternativo di innovazione e di business, in grado di influenzare e orientare le aziende della Silicon Valley e incidere sulla nascente *sharing economy*. Tuttavia, la globalizzazione della circolazione dei dati ha dimostrato che a livello istituzionale c'è bisogno anche di politiche strategiche per la creazione di infrastrutture europee per la gestione dei dati poiché ciò viene ad incidere direttamente sull'applicazione della regolamentazione europea dei

dati. La Cina, ad esempio, ha prestato grande attenzione all'ubicazione dei server e dei database, provvedendo alla costruzione della propria sovranità sui dati nonostante un modello atipico di protezione della privacy, forte nel settore privato e quasi inesistente per quanto riguarda il settore pubblico. Il mercato europeo invece è caratterizzato da una debole sovranità sui propri dati a fronte di un mercato dei dati che spesso tende a mandare i dati all'estero dove le leggi sui dati sono più deboli e vigono standard molto più bassi. Ciò ha portato ad una crescente pressione per avere un cambiamento nelle policies regolatorie europee sui dati (in questo senso si vedano la Direttiva sull'uso secondario, la proposta Chat control 2.0 ecc.). La sfida principale per l'Unione Europea oggi è quindi quella di investire sui propri asset istituzionali, costruendo le condizioni per la sovranità sui dati che non porti a smantellare l'attuale regolamentazione dei dati ma crei una migliore integrazione tra questi.

Keywords

Global Circulation of Data; Data Protection; Europe; Data Localisation; Rights-Based Sovereignty.

Circolazione globale dei dati; protezione dei dati; Europa; localizzazione dei dati; sovranità basata sui dati.