universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„ Privacy and Security in Focus: Comparative Study of the EU GDPR and UK Data Protection Laws in Safeguarding Data in the Digital Age "

verfasst von / submitted by

Guillaume SORRELL

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Advanced International Studies (M.A.I.S.)

Wien 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt Postgraduate programme code as it appears on the student record sheet:	A 992 940
Universitätslehrgang lt. Studienblatt Postgraduate programme as it appears on the student record sheet:	Internationale Studien / International Studies
Betreut von / Supervisor:	Prof. Stephan Wittich

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

1) Abstract, Zusammenfassung:

This comparative study between the EU and the UK's legal frameworks for data protection, the EU GDPR and the UK Data Protection and Digital Information 2 Bill, explains the legal origins of the notion of privacy, before contrasting the effectiveness of both legal frameworks in protecting privacy and security by providing a detailed explanation and analysis to highlight their respective strengths, weaknesses, and threats to data privacy and security. This thesis underlines how the plethora of amendments to the UK GDPR and DPA in the DPDI2 bill follow a trend of concession of Henry the VIIIth powers to the Secretary of state and Law enforcement as well as an opacification of the current laws which, under the guise of ease of compliance, innovation and security ultimately undermine the current data privacy framework in favour of heightened, widespread nation-wide processing of sensitive public data for unclear, unmandated use.

Diese vergleichende Studie zwischen den Datenschutz-Rechtsrahmen der EU und des Vereinigten Königreichs, der EU-Datenschutz-Grundverordnung (GDPR) und dem britischen Gesetzentwurf über Datenschutz und digitale Informationen (Data Protection and Digital Information 2 Bill), erläutert die rechtlichen Ursprünge des Konzepts der Privatsphäre, bevor sie die Wirksamkeit beider Rechtsrahmen beim Schutz der Privatsphäre und der Sicherheit gegenüberstellt. In dieser Arbeit werden die Unterschiede zwischen der EU-DSGVO und den zahlreichen Änderungen im DPDI2-Gesetzentwurf hervorgehoben.Dem Trend folgend, die Befugnisse Heinrichs des Achten an den Staatssekretär und die Strafverfolgungsbehörden zu delegieren und bestehende Gesetze zu verschleiern, untergräbt der DPDI2-Gesetzentwurf letztlich den aktuellen Datenschutzrahmen zugunsten einer verstärkten, weit verbreiteten landesweiten Verarbeitung sensibler öffentlicher Daten für eine unklare, nicht vorgeschriebene Verwendung.

On my honour as a student of the Diplomatic Academy of Vienna, I submit this work in good faith and pledge that I have neither given nor received unauthorized assistance on it - Guillaume Sorrell

Table of Contents

Introduction

Data collection has engrained itself as a vital segment in today's society as it allows organizations to make informed decisions and improve their operations. The increasing use of data in various industries, such as healthcare, finance, and technology, has led to significant advancements and efficiencies. However, the collection and use of data also raise important privacy and security concerns. As more data is collected and shared, there is an increased risk of data breaches and misuse of personal information. It is crucial for organizations to implement strong security measures and for individuals to be aware of their rights and how their data is being used. Additionally, there are various laws and regulations that organizations must abide by to ensure the protection of personal data.

Some specific examples of how data collection is used in various industries and the implications for privacy and security include, but are not limited to:

Healthcare: Electronic health records (EHRs) and wearables allow for the collection of large amounts of personal health data. This data can be used to improve patient care and population health, but it also raises privacy concerns, such as the risk of unauthorized access to sensitive information.

Marketing: Data on consumer behaviour and preferences is collected through various means, such as cookies on websites and mobile apps. This data is used to personalize advertising and improve the customer experience, but it also raises concerns about the extent to which companies can track individuals' online activities.

Finance: Data analytics is used to identify fraudulent transactions and assess credit risk. Personal financial data is also used to offer personalized financial products and services, but it also raises concerns about the security of sensitive financial information and the potential for discrimination.

In all these examples, it is important for organizations to have appropriate security measures in place to protect personal data, and to be transparent about the data they collect and how it is used. Additionally, individuals should be aware of their rights,

such as the right to access and correct their personal data, and to make informed decisions about the use of their data.

The Data Protection and Digital Information Bill 1, published by the Department for Digital, Culture, Media and Sport (DCMS), was introduced into the UK Parliament on 18 July 2022. In line with the conclusions reached by the Government (23rd of June 2022) following the public consultation Data: A New Direction (10th of September 2021 – 19th of November 2021), the Bill introduces a number of significant changes to the UK's personal data protection legislation, which until now has closely mirrored the GDPR, in order to take a more flexible and pragmatic approach.

Following Brexit, the UK passed a law providing for the continuation of directly applicable EU legislative measures in UK law, including the GDPR. This legal transposition did not stop at mere textual identity, in the sense that it was also agreed that the retained EU legislative measures should be interpreted in accordance with the relevant case law of the CJEU (Court of Justice of the European Union), and the general principles of EU law.

Thus, the legislation governing the protection of personal data in the UK has been found to be strictly identical to the EU legal framework since Brexit. This justified the adequacy decision taken by the European Commission on the 28th of June 2021, allowing the free movement of data between the European Union (hereinafter, EU) and the United Kingdom, the level of data protection being naturally considered adequate in this country.

However, the UK was quick to indicate its intention to set a new direction for its data protection legislation. The public consultation Data: A New Direction at the end of 2021 already made clear the desire to transform the UK's data protection rules to make them less restrictive, and to foster innovation and growth.

As a result, the “Data Protection and Digital Information Bill 1”, presented to Parliament last summer was withdrawn by Secretary Donelan, whom introduced the Data Protection and Digital Innovation 2 bill on the 8th of March 2023, which in turn gives concrete expression to this desire to simplify and make the data protection rules more flexible. This new bill, however, creates several divergences with the GDPR.

Many elements and proposals of the British text indeed introduce significant differences, both conceptual and practical, between the two legal orders.

This will to reduce burdens on organisations while maintaining high data protection standards on behalf of the UK government begs the following question:

How does the legal framework of data collection in the UK and the EU differ and what are the implications for data privacy and security?

In order to compare and contrast the legal frameworks for data collection in the UK and the EU, and to evaluate their effectiveness in protecting privacy and security, the following general sub-questions must equally be addressed:

a. What legal principles underpin data privacy and security in both legal frameworks?
b. What are the strengths, weaknesses and threats of both legal frameworks?
c. What are the practical implications of the legal frameworks for individuals, businesses and society?

Part I: The evolution of the concept and legislative framework of data protection

I. The origins of data protection as a manifestation of the right to a private life.

In order to understand the origin and content of the right to the protection of personal data we must first go back to the right to private life or privacy, of which it is a manifestation.

The right to privacy did not take shape as an autonomous right until the last decade of the 19th and the beginning of the 20th century, although some of its manifestations, such as religious freedom, have had some isolated positive recognition since antiquity, in the Edict of Milan in 313, by the emperors Constantine and Lucinius[1]. In the Middle Ages it appears in the work of St. Augustine and, in the form of "peace of the house" or, as it was referred to across the United States in more than 250 court rulings in the late 18^{9th} century, "sacred privacy of domestic life"[2].

Later, in the modern age, other forms such as freedom of conscience, confidentiality of communications and bodily privacy appear, although the latter respond more to the idea of security than to that of privacy[3].

As society evolves, mainly within the framework of the rule of law and the protection of the individual against the power of the state, the expressions described above give rise to a new value worthy of legal protection: it is a sphere or area of people's lives in which religious feelings, the family home and private correspondence are included, but also other elements in respect of which there is a need to preserve for oneself. This feeling or need evolved into an autonomous right in American case law of the early twentieth century: the right to private life or privacy, which later became part of international declarations of rights[4]. Instruments such as the Universal Declaration of

[1]. Dură, Nicolae V (2019), *About the Freedom of Religion and the Laicity. Some Considerations on the Juridical and Philosophical Doctrine*, Bulletin of the Georgian National Academy of Sciences, Tbilisi, p. 157
[2] Gajda, Amy (2022), *Seek and hide: the tangled history of the right to privacy*, Viking, New York, p.27
[3] Richardson, Megan (2017): The Right To Privacy: Origins And Influence Of A Nineteenth-Century Idea, Cambridge University Press, Cambridge, p.90
[4] Gajda, Amy (2022), *Seek and hide: the tangled history of the right to privacy*, Viking, New York, p.9

Human Rights of 1948 (Article 12), the European Convention on Human Rights of 1953 (Article 8), the Covenant on Civil and Political Rights of 1960 (Article 17), contain provisions that elevate the protection of the privacy of individuals to the status of a fundamental right[5].

Thus, Article 12 of the Universal Declaration of Human Rights guarantees that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation"[6], from which it can be inferred that the rights to inviolability of the home, confidentiality of correspondence, honour and reputation form part of the right to privacy within the scope of this instrument.

For its part, Article 8 of the ECHR in paragraph one ensures that "everyone has the right to respect for his private and family life, his home and his correspondence"[7]. In paragraph two, it directs this protection exclusively against interference by public authorities in these areas, which may only be carried out if it is provided for by law and constitutes a measure which, "in a democratic society, is necessary for national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

In other words, it must be justified, among other reasons, by an exhaustive list of public interests. Although this protection is *a priori* exclusively directed against state interference, the European Court of Human Rights gives a broad interpretation to the right to private life or privacy, extending protection to attacks from individuals or persons under private law and to certain elements related to a person's identity, such as his or her name and personal image, as well as his or her physical and moral integrity[8]. The Court itself has stated that Article 8 of the ECHR imposes positive obligations on the State to adopt the necessary measures to guarantee the protection of this right, among which is that of finding a balance between the right to privacy

[5] Ibidem, pp 192-194
[6] United Nations, *Universal Declaration of Human Rights*, 1948 (article 12, §1)
[7] Council of Europe, *European Convention on Human Rights*, 1950 (article 8, §1)
[8] Rubio Dosamantes v. Spain, 21/02/2017, paragraph 26, http://www.bailii.org/eu/cases/ECHR/2017/200.html

and freedom of expression, protected by Article 10 of the ECHR[9], which in turn, in its paragraph two, provides that the State must adopt the necessary measures to guarantee the protection of the right to privacy. This article, in its paragraph two, provides that the state may limit freedom of expression under conditions similar to those we have already transcribed from article eight, paragraph two, to which is added that of "preventing the disclosure of information received in confidence"[10], a provision which the European Court of Human Rights interprets as including the protection of the private life or reputation of individuals. The Spanish Constitutional Court has also had occasion to rule on this issue, stating that the right to freely communicate information may be limited by the right to personal and family privacy, even in the case of public persons[11].

Like many of the fundamental rights set out in these and other international instruments, the right to privacy is a natural corollary of the recognition of human dignity and is indistinguishable from the right to the formation of one's personality[12].

According to Italian jurist and Professor Giancarlo Rolla[13], the evolution that the constitutional protection of privacy has undergone ranges from the first stage in which it was considered a right of a negative nature "closely linked to the right to property or *ius excludendi alios*", which focuses on the right not to suffer external intrusions, to another of a positive nature "which becomes aware of the impossibility of remaining unaware of the information process activated by the impressive acceleration of technological innovations", such as the power to define one's own personality or identity by controlling the circulation of data related to oneself.

However, the context in which the concern for the protection of personal data begins to take shape spawns in the mid-twentieth century, a period in which the advance of technology begins to produce the first computers and programmes for processing data. Those are mostly reserved for civil and commercial use, on a large scale and with

[9] Ibidem, paragraph 27
[10] Council of Europe, *European Convention on Human Rights*, 1950 (article 10, §2)
[11] *Spanish Yearbook of International Law Online* 1, 1, 197-238, sentence 197/1991, 17/10/1991 **https://doi.org/10.1163/221161291X00096**
[12] Ibidem
[13] Rolla, G. (2001), *The difficult balance between the right to information and the protection of dignity and private life. Brief considerations under the light of Italian experience*, In Law and Person, no. 44, pp.263-269.

predictive effects on the behaviour of individuals, such as the forecasts for the US presidential elections of 1950 and 1960 highlight. In 1968, IBM electronics introduced the first database management system[14], both technical and personal, whose computer processing multiplied exponentially the use of this information and, as a consequence, the possible infringement of individual rights. Thus, at the end of the sixties and the beginning of the seventies, concern began to emerge in the American doctrine regarding the threat that computerised processing of personal data represented for the private life of individuals, a concern that deepened as the use of the technique developed and spread. Entailing this concern, the first data protection regulations began to emerge, although not in the United States, but rather in Europe, with the Datenschutzgesezt of the German Land of Hesse in 1970 and the Data Lag of Sweden in 1993. These regulations specifically referred to files of a public nature, due to the fact that the use of computers by the private sector in Europe had not yet become sufficiently widespread to constitute a threat to the rights of individuals.

In 1998, the Council of Europe had issued Resolution 509, aimed at highlighting the possible confrontation between human rights and the new scientific and technical achievements of commerce, which was followed in subsequent years by two other resolutions of the Council of Europe's Ministerial Council[1516] aimed at recommending member states to "take certain precautions to prevent the misuse or abuse of personal data contained in commerce data banks", both in the private and public sector.

It is within this organisation that, at the beginning of the 1980s, the first international instrument on the protection of personal data was signed, Convention 108[17].

In short, we can attribute the formation of the right to the protection of personal data, which finds its roots in the right to privacy and dignity, to the evolution of information technology and communications, although the first of the aforementioned rights later acquired autonomy when it was configured as a guarantee for the protection of other

[14] Fry, James P. & Sibley, Edgar H. (1976), *Evolution of Data-Base Management Systems*, ACM Computing Surveys, Volume 8, Issue 1, pp.7-42.
[15] Council of Europe's Ministerial Council (26/09/1973), resolution nº73, on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector
[16] Council of Europe's Ministerial Council (20/09/1974), resolution nº74, on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector
[17] Council of Europe (28/01/1981), *Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data*.

fundamental values[18]. For it became evident that the generalisation, facilitation and acceleration of the processing and, especially, of the combination, use and communication of personal data by third parties allowed the latter to invade the intimate or private sphere of the individual's life. That is, what one wishes to keep to oneself alone, that which one also wishes to keep from the knowledge of other persons or of persons outside one's closest circle.

Therefore, it is this privacy or intimate sphere that is protected through the control of personal data because a publicly known but isolated piece of data may be innocuous, but put in connection with more data also disclosed to the public or third parties can reveal a person's intimate profile.

II. The concept and limitations of data protection as a legal doctrine

In Europe, as has happened with other fundamental rights, it was case law that began to consider the protection of personal data as a right implicit in the right to privacy when there were still no specific rules regarding the matter. This implicitness was therefore protected by international conventions and national constitutions with the status of a fundamental right. Thus, both the jurisprudence of the European Court of Human Rights and the constitutional courts of the European States gradually recognised the protection of personal data as a fundamental right, based on Article 8 of the ECHR, which we have analysed in the previous section.

However, as we have previously discussed, it wasn't at least until the middle of the 20th century that the right to privacy manifested itself in freedom of religion and conscience, the inviolability of the home and the confidentiality of communications in its positive version. It was not until after that time that demographic growth, the modernisation of the State and public administrations and technical advances began to extend the processing of personal data, which gave rise to the right to the protection

[18] De Terwangne, C. (2011), *Internet Privacy and the Right to be Forgotten/Right to Oblivion*, Internet, Law and Politics Magazine, pp.1-13

of personal data or, as stated in international and European instruments, to the protection of natural persons in relation to the processing of their personal data.

The right to the protection of personal data consists in granting protection to natural persons so that they are not invalidated in an unwanted way through the use of their personal data or more precisely, as defined by the Constitutional Tribunal of Spain[19]: "consists in a power of disposal and control over personal data which empowers the individual to decide which of those data to provide to a third party, be it the State or a private individual, or which may be collected by that third party, and which also enables the individual to know who holds those personal data and for what purpose, and to object to such possession or use […], powers of disposal and control which are legally embodied in the power to ensure the collection, acquisition of and access to personal data, their subsequent storage and processing, as well as their use".

This definition of the Constitutional Court of Spain contains the essential elements of the protection granted by this fundamental right to the data subject: knowledge or information and powers of control, disposal and opposition, since in addition to its negative aspect (the exclusion of third parties from the individual's sphere of privacy), personal data protection also has a positive form in the so-called right to informational self-determination, which consists of control over one's own data or over the information generated by a person.

It should be noted that the protected subject is always a natural person, and the protection extends to data that apparently does not have the capacity to identify him or her but which, if processed according to certain guidelines, could invade the sphere of personal privacy as we mentioned in the previous section.

In this sense, the Court of Justice of the EU (CJEU)has declared that a static IP address constitutes personal data, as it allows the identification of the user[20]; but it has also declared a dynamic IP address to be protected personal data in certain circumstances[21]. It has also stated that communications metadata is also personal data and therefore

[19] Ombudsman of the People v Attorney General, Constitutional appeal, STC 292/2000, ILDC 128 (ES 2000), 30th November 2000, Spain; Constitutional Court
[20] Scarlet Extended SA v Sabam (24/11/2011) (C-70/10) EU:C:2011:771
[21] Breyer v Germany (19/10/2016) (C-582/14) EU:C:2016:779

deserves the protection granted by articles 7 and 8 of the Charter[22]. It is one of those rights susceptible to limitations or restrictions established by a legal or similar rule, always subject to certain specific requirements and to a restrictive interpretation, such as those established in Article 8.2 ECHR, which we have already analysed.

On the other hand, the right to the protection of personal data is a fourth generation right or one of the categories of cyber rights, as other authors call them[23].

Godwin, in addition to sharing this classification, defines this fourth generation by the elements that characterise it, among which he cites the emergence of new values, rights and social structures (which require a new repertoire of ethical principles), new forms of human interrelation through technology and new virtual communities that are not bound by territory or a common language[24]. The protection granted by this type of rights arising from the new technologies extends beyond privacy, to also cover other fundamental values such as personality, the construction of one's own identity or honour - in a broader sense, other freedoms such as freedom of expression and ideology are also protected, as well as the exercise of political, economic, educational and labour rights.

Therefore, the content of the right to the protection of personal data has been distributed in four generations. In these four generations, the content of this right varied from a focus on protection against unlawful use of personal data exclusively by public authorities, based on a geographically localised aspect and restrictions on access and use, to the current situation in which protection is directed both at the use of personal data by private individuals and by public bodies and transcends any geographical scope.

[22] Joined cases, Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärnter Landesregierung (C-594/12)
[23] Godwin, M. (2003) Cyber Rights: Defending Free Speech in the Digital Age. MIT Press, London, 10, p.77
[24] Ibidem, pp. 1-23; 70-77;

Like many other fundamental rights, the protection of personal data collides with other rights and freedoms: freedom of expression and information, freedom of enterprise and intellectual property. The European regulation establishes some basic rules to resolve this conflict, although it will be up to the law and the authorities of each State Party to provide a concrete solution to the problems that arise in practice, for which they can rely, in addition to the provisions of the regulation, on the case law of the Court of Justice of the EU[25].

As has always been the case in the history of law, the rule appears once the need for a specific protection is perceived in society and, in this sense, the protection of personal data is a recent right that did not emerge until the development of technology made special protection necessary in the face of the ease and speed with which personal information about individuals is collected, combined, used and communicated, which constituted an intrusion into the most intimate sphere of individuals, which was not previously the case.

Therefore, when this threat was recognised by both doctrine and case law, the tool available at that time was used to respond to it, which was the right to privacy. The protection of personal data became another manifestation of it, along with the inviolability of the home and of communications among others.

Since its gestation in doctrine, case law and later in positive law, the protection of personal data has been a right in continuous evolution, as it will continue to be as long as technology continues to evolve and new forms of processing personal data continue to be discovered.

We can give as an example of this evolution social networks, which we consider to be marking a new generation in the evolution of the right to the protection of personal data and, especially, in the concept of private life coined by the new generations, who make a large part of their lives public by exposing them on social networks and blogs. One could argue that these behaviours are not incompatible with the idea of privacy, but rather redefine it, since the desire to share certain aspects of one's private life with the public does not exclude the interest in protecting the sphere in which one's

[25] Case law Scarlet Extended SA v Sabam, for example

personal decisions are made, which is generally made public in an unconscious way and in which one does not wish to allow outside interference.

To conclude this section, we will add that other new forms of data processing relating to a person are artificial intelligence and Big Data, which can allow those who use them to predict what decisions will be taken by subjects in certain circumstances, i.e., to know aspects of the person of which he or she is not even aware. These predictive operations based on the combination and analysis of the information produced by a subject are called profiling and are particularly protected by European regulation.

Special mention should be made of the technology known as the internet of things, which consists of "things" (toys, household appliances, cars, etc.) that are connected to the internet and programmed to carry out data processing without human intervention. Such processing may include the collection, storage, classification, combination of personal data and, more worryingly, communication of personal data to third parties. This technology deserves particular attention as it involves the roles of data controllers, as many people are involved in its production and marketing, which in turn may not coincide with the recipient of the data who may carry out other independent processing operations on the data.

Personal data protection provisions must therefore be sufficiently open, consistent and relevant to ensure that data is not left unprotected because the status quo does not always provide for such cases. These dispositions must therefore also be prepared to shield from future technologies that may emerge without the luxury of being able to presently fathom them.

III. Its relationship with international law and the territorial aspects of law

With the advance of virtual environments, it is therefore relevant to argue that the territory is losing importance, not only as a binder of communities but also as a dimension in which human relations are embodied. Floridi argued that the virtual environment makes the territory lose meaning as human interactions no longer require physical presence, which means that "the territory is deterritorialised through cyberspace, even if only momentarily"[26], as we see that interactions in this sphere are influenced at the same time as they influence the physical spatial dimension, which leads him to conclude that the knowledge that computers and telecommunications spread throughout the world "is not a tool for describing reality, but for constructing it"[27].

However, one could argue against this author when he alludes to the relational, social, cultural and political dimensions centred on cyberspace as new territorial spaces. This is not a new form of "territorialisation" or "re-territorialisation" but new dimensions devoid of territory.

Territory has historically and from a legal point of view been the geographical sphere in which the national legal systems of independent states govern, exercising power within their territory in a sovereign manner, excluding interference from other states. Notwithstanding this, there are intermediate situations in which states apply the law of another state within their territory, usually for specific cases or situations[28]. Situations that fall under the scope of private law and whose solution requires the rules of a specific legal system to be transcended are the subject of private international law, a branch of law that applies to legal relationships in which there are elements or connections of sufficient intensity that relate it to more than one legal system[29] or, in

[26] Floridi, L (2014): The fourth revolution : *How the infosphere is reshaping human reality*. Oxford University Press, Oxford

[27] Ibidem, p.233

[28] Vashist, A. (2021), Theory of Extraterritoriality of States and Jurisdiction in International Law, Legal Service India, E-Journal, Raffles University Neemrana

[29] Kramer X. , Rooij M. de, Lazic V. , Blauwhoff R. , Frohn L. (2012) *A European Framework for private international law : current gaps and future perspectives*, Directorate General for Internal Policies, Policy Department C : Citizen's rights and constitutional affair, European Union p.68

other words, when a matter is related to the legal systems in force in different territories.

The major source in this branch of law is the conflict rules, which are those that provide a solution to a case by means of an indeterminate choice of national substantive law or of a foreign substantive law[30]. This type of rule consists of three parts: the category or description of the situation, the point of connection (which is the element chosen to determine the applicable law) and the legal consequence, which in this type of rule is always the application of a specific legal system, which may be the *lex fori* or another foreign system[31]. These rules that order the application of a different law are called rules of renvoi and, unlike substantive law, they do not resolve the merits of the case but refer to the source from which the rule must be drawn for its resolution[32]. Within private international law we find, in addition to the conflict rules, the rules of police, which are those that exclude the operation of the conflict rules to the cases that fall under the scope of application delimited by the factual assumption described, giving this a solution of substantive law.

As we will see in the development of this research, data protection law contains both public and private international law provisions, especially in the following aspects:

- as a fundamental right, it is part of international fundamental rights law, especially since 1981, through the Council of Europe Convention No. 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data (hereinafter referred to as Convention 108).

- The subject protected by the provisions of this law is a natural or private person and the legal relationships that make up its object in a large number of cases contain elements that relate them to more than one legal system, and therefore fall under the scope of private international law.

[30] Ibidem, p.64
[31] Ibidem, p.49
[32] Ibidem, p.46

- Given that a protection of personal data that is limited to connections exclusively with the territory of the EU would allow fraud of law very easily, some rules seek to transcend the territorial scope of application of the law.

All of the above regarding the territorial validity of legal systems and the relations between them takes on a different dimension in the rights derived from the new technologies, among which is that of personal data protection, since most of the processing of personal data and the legal relations captured by data protection law do not take place in a specific geographical space but in cyberspace.

Or, to put it another way, connecting these situations and relationships with a territorial element that is the presupposition of national law and the rules of renvoi does not correspond to reality, due to the ubiquity of electronic connections and the multiplicity of elements with different geographical locations that can become part of a virtual legal fact. In order to fully understand the issues related to the territorial aspects of cyberlaw, it is necessary to establish a definition or, at least, a characterisation of the virtual space or cyberspace to which we have referred.

According to Encyclopaedia Britannica, cyberspace is an "amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links. It exists, in the perspective of some, apart from any particular nation-state."[33]

Cyberspace is therefore an intellectual creation, an entelechy to define the operations carried out with the intermediation of the Internet or the network that nowadays connects millions of devices behind which, in most cases but not always, there are people and that allows (among other actions) to find, generate, transmit, exchange and publish information or data that are physically located anywhere in the world, from any other point of the globe. For cyberspace there are no borders[34]. Notwithstanding this, actions performed in "virtual space" can have effects (legal or otherwise) on "real

[33]Brussel, J (2013) Definition of "*cyberspace*", Encyclopaedia Britannica

[34] However, there could exist some type of border through geolocalisation, a virtual process which could offer differentiated virtual content depending on the geographical location from which one consults the Internet. The European Union is for example developing a strategy against discrimination based on this process, strategy which engrains itself in the path to a common digital market.

life". Some legal effects of virtual operations are electronic banking operations, contracts that can be signed electronically (the most frequent being the sale and purchase of goods or products online, to be sent to the buyer's home) and even criminal acts such as "cyberstalking", in which the victim suffers in real life the consequences of the actions of other people in virtual space.

Lastly, the right to the protection of personal data, as it also involves regulation of new technologies, is affected by the regulatory disconnect that Abbot denounces, consisting in the fact that science and technology develop at a much faster speed than the adoption of new regulations, although it is imperative that regulatory frameworks are able to match this speed[35]. This author postulates that for more than two decades the idea of regulatory control as an exclusively state activity has been changing, and that we are now in a "post-regulatory" stage, in which actors such as industries, NGOs, consumer associations, industry associations and financial institutions have resources and capacity that allow them to improve the regulatory process and are willing to use them.

[35] Abbot, C (2012) Bridging the Gap – *Non-state Actors and the Challenges of Regulating New Technology*, Journal of Law and Society, Vol. 39, no, pp. 330-359

Part II: The General Data Protection Regulation's implementation: change woven into consistency.

Introductory remarks:

Article 8 of the ECHR provides, as we have seen, as well as article 16 of the Treaty of the European Union (hereinafter, TEU), that "Everyone has the right to respect for his private and family life, his home and his correspondence". In essence, this is one of the innovations introduced by the Treaty of Amsterdam in 1997, whose symbolic significance will be reinforced by its codification in the Charter, which will have the same legal value as the Treaties with the Treaty of Lisbon.

However, the first EU text to address the issue of personal data protection predates these primary legal texts by several years. It was with Directive 95/46/EC of the 24th of October 1995[36], an instrument of secondary legislation, that EU law took up this new issue, first raised by the Council of Europe in the 1970s as previously delved into[37].

Failing to base itself on the Treaties or the Charter, Directive 95/46/EC made use of the traditional provision concerning the "approximation of laws" between EU Member States with a view to edge closer to completion of the internal market . It is therefore on the foundation of this legal basis that the Council, acting under the "co-decision" procedure, has been able to develop a whole body of legislation laying down the first principles and objectives concerning the Community vision of personal data protection.

The need to justify this intervention by the EU as part of the completion of the internal market, without which the directive would have been devoid of any legal basis, shapes the underlying concept of personal data protection. The aim is not simply to protect individuals against any infringement of their right to respect for their personal data,

[36] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[37] See Part 1 Section 3: Its relationship with international law and the territorial aspects of law: Regarding Resolutions no. 73 and 74 of 1973 and 1974 respectively by the Council of Europe's Ministerial Council, the Council of Europe adopted on the 18th of January Convention 108.

but also, and perhaps above all, to ensure common standards of protection in all Member States, in order to allow the free circulation of such data and thus facilitate the completion of the internal market. It is therefore that "whereas data-processing systems are designed to serve man; whereas they must […] respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals"[38], the fact remains that, "given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy"[39].

Although this directive, which was largely inspired by Swedish[40], German[41] and French[42] legislation set out the main principles and objectives for the protection of personal data within the EU, its form nevertheless appeared to be open to improvement. The need to rework personal data protection issues has been highlighted by the development of the digital economy, the European Commission's objective of creating a single digital market[43] and the new challenges posed by the collection of data, particularly for the purposes of preventing terrorism or criminal offences[44].

EU institutions therefore worked to replace Directive 95/46/EC. This was achieved on 27 April 2016, with the adoption of Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This text, a central element of the "personal data" legislative package, is accompanied by two directives, one on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data; and the other

[38] TEU, article 114
[39] Directive 95/46 EC, Recital 9.
[40] Swedish Data Act (SFS 1973:289) 11 of May, 1973
[41] German Federal Data Protection Act of 1977 : Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act -. BDSG)
[42] French Law no. 78-17 of 6th of January 1978 on data processing, data files and individual liberties
[43] President Juncker's political guidelines presented during the opening speech of the plenary session of the European Parliament on 15 July 2014 in Strasbourg.
[44] Ibidem.

on the use of Passenger Name Record (PNR) data for the prevention, investigation, detection and prosecution of terrorist offences and serious crime[45].

It should be noted that the main principles of the GDPR are directly in line with those of the directive it replaces. At the same time, the EU legislator has seized the opportunity presented by this text to generate real added value compared with Directive 95/46/EC.

[45] Directive dealing with personal data protection issues for which the Area of Freedom, Security and Justice is responsible.

I. The GPDR: towards a greater guarantee of the right to the respect of personal data

Firstly, a major change brought about by the GDPR is the choice of the regulation as the legislative instrument, whereas previous provisions on personal data protection were based on a directive. This change of form has important legal consequences, as the choice for a regulation highlighted a will to combat the disparities in legislation within the Union.

It should be reminded that Article 288 of the Treaty on the Functioning of the European Union (hereinafter, TFEU) states that a regulation has a "general application". It is "binding in its entirety and directly applicable in all Member States"[46]. This is in contrast to a directive, which is "binding, as to the result to be achieved, upon each Member State, to which it is addressed, but shall leave to the national authorities the choice of form and methods."[47]

The regulation thus offers individuals the possibility of relying on the "full" direct effect, i.e. both vertical and horizontal, of its provisions before the national courts[48]. This guarantees greater unity of EU law in that, as soon as the regulation enters into force, every citizen of the Union can rely on the same rights in every Member State, thanks in particular to the regulation's particularly comprehensive form of invocability. Furthermore, the unity of EU law is also strengthened by the fact that the text of the regulation applies directly in each and every Member State. It makes no difference whether an article of the regulation is invoked in Hungary or in France. The provisions are the same.

However, this is not guaranteed with the instrument of the directive. Although the same directive applies in all Member States, the latter are free to transpose its provisions as they wish, as long as the objectives set by the directive are achieved.

[46] TFEU, article 288§2
[47] TFEU, article 288§3
[48] Politi s.a.s. v Ministry for Finance of the Italian Republic (14/12/1971), Court of Justice of the European Communities, C-43/71

This latitude left to the Member States can lead to a certain fragmentation of the law between Member States, even though a directive sets the same objectives to be achieved. This is what the European legislator criticised when drafting the GDPR in recital 9: "The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity" [49].

Nonetheless, the choice of regulation is not a universal remedy for the fragmentation of the law. Indeed, because of the difficulty of obtaining a consensus between the Member States and the EU institutions on new data protection legislation, no fewer than 56 articles or recitals of the GDPR leave the Member States a certain amount of room for manoeuvre, thereby considerably reducing the ambition for greater unification of Community law on the protection of personal data.

Finally, the nature of the legislative instrument chosen, i.e. the regulation, is accompanied by another change, that of the legal basis of the text. Unlike the 1995 Directive, which relied on provisions relating to the approximation of laws to complete the internal market, this time the GDPR is based directly on primary law. Explicit reference is made to the Treaties[50], but also to the Charter[51].

Secondly, and while the GDPR does not generally reinvent the law on personal data, as it is in line with continuity and reaffirms many of the principles of the 1995 Directive that it repeals, it does enshrine a number of new rights with regard to the protection of personal data.

This is particularly true of the right to data portability[52]. This right gives data subjects the possibility to "receive the personal data concerning him or her, which he or she

[49] EU GDPR, Recital 9
[50] TFEU, Article 16, Recital 1
[51] ECHR, Article 8, Recital 1
[52] GDPR, Article 20, Recital 68

has provided to a controller, in a structured, commonly used and machine-readable format" and to "have the right to transmit those data to another controller"[53].

In particular, this new right means that individuals can no longer be prisoners of a data controller who refuses to return their personal data in order to keep them captive to a certain product or service (software, for example). By enshrining this right to portability, the GDPR facilitates competition between data controllers.

Another new feature is the notion of *digital majority*[54]. The idea is not to set an age limit below which digital minors would not be able to use digital services, as such a measure would be relatively complex to implement. Rather, the age set by the GDPR for digital majority is in fact intended to provide mechanisms offering better protection for digital minors and their rights with regard to their personal data. According to the letter of the GDPR, minors under the age of 16 are not considered to have been able to consent to the collection of some of their data in the context of the use of information society or digital services. The immediate consequence for the data controller is that such data collection is entirely unlawful. They are therefore not authorised to process such personal data. However, this numerical majority is one of the many provisions in respect of which the Member States have some room for manoeuvre. The GDPR sets the age of consent at 16, but allows it to be lowered to 13. France, for example, has chosen to set the age of digital majority at 15[55]. Below this age, the consent of one or more holders of parental authority is required in addition to that of the minor[56].

As was the case under the 1995 Directive, the role of consent under the GDPR remains central if the processing of personal data is to be recognised as lawful[57]. This element, which lies at the heart of the legislation, is reaffirmed and illustrates the idea of the

[53] GDPR, Article 20§1
[54] GDPR, article 8
[55] French Law of the 06/01/1978 relative to data processing, data filing and individual liberties, modified. Article 45§1
[56] Ibidem, Article 45§2
[57] Article 6 of the GDPR sets out six conditions, the first of which is consent, under which processing can be considered lawful. Of these six assumptions, only consent is the subject of a specific article within the GDPR, namely article 7.

GDPR's increasing power while retaining the main principles of personal data protection laid down by the 1995 Directive.

Another innovation worth noting is the possibility of collective action to facilitate the exercise of the rights enshrined in the GDPR[58]. However, the rights of access, opposition, information on processing or erasure ("right to be forgotten") are only reaffirmed by the text and already featured in the 1995 Directive[59] or in pre-existing case law[60].

The growing importance of the right to protection of personal data has also been made possible by a better definition and reorganisation of the roles of the various players involved in "data". Let us delve into this idea in the second section of this second part.

[58] GDPR, Article 80

[59] Directive 95/46/CE: Article 12 (right of access); Article 14 (right to object); Articles 10 and 11 (right of information)

[60] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González (13/05/2014) case C-131/12 regarding the right to be forgotten

II. A reorganisation of the relations between actors and data

In addition to the individuals concerned by the collection and processing of their personal data, i.e. data subjects, we can note two main players: those responsible for data processing on the one hand and the supervisory authorities on the other. With the advent of the GDPR, the former find their obligations broadened, entailing a heightened degree of necessary responsibility, while the latter are given new powers of control and sanction.

Let us first examine, on the one hand, the modalities of the responsibility of said data processors:

In this respect, the major paradigm shift is that it is no longer up to the supervisory authorities (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in Germany, or the Integritetsskyddsmyndigheten in Sweden, for example) to demonstrate that a player is in breach of data protection legislation. It is now up to that actor, i.e. the data controller, to prove that his processing activities comply with the GDPR[61]. We are witnessing a reversal of the burden of proof. This does not simplify the process, particularly for economic operators, especially as demonstrating compliance is never a foregone conclusion, but must be a long-term process. To limit uncertainty in this area, certification mechanisms[62] or codes of conduct[63] can be used. These elements alone do not seem sufficient to prove compliance with the GDPR, but they do demonstrate a willingness on the part of the data controller to comply[64].

The downside of this reversal of the burden of proof is that those collecting and processing personal data are now largely exempt from any prior notification to the

[61] GDPR, Article 24: "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation"

[62] GDPR, Article 42

[63] GDPR, Article 40. It is worthy of not that Directive 95/46/CE encouraged in its article 27 the redaction of such codes of conduct.

[64] GDPR, Article 24§3: "Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller"

supervisory authorities, even though this notification system was a key feature of the 1995 Directive[65].

Thus, under the GDPR, and in line with the 1995 Directive[66], the only mechanism remaining is prior consultation with the supervisory authority for certain personal data processing operations, where impact assessments carried out by the controller - which is sometimes mandatory[67]- have revealed a particular threat to the rights of the individuals concerned[68]. If the supervisory authority is to detect a breach of the GDPR, then a broad selection of powers is made available to it, such as prohibiting the processing or imposing administrative penalties[69]. Although prior notification is no longer required for processing operations that have little impact on the rights of the data subjects, the prior consultation mechanism still targets the most sensitive or large-scale processing operations, giving the supervisory authorities real means of action.

However, the scope of exchanges between data controllers and supervisory authorities remains much broader. In particular, the GDPR stipulates that data controllers must report any data processing malfunction "as soon as possible"[70]. Another example of this close and necessary cooperation is the role of the data protection officer[71], who acts as a link between the data controller and the supervisory authority.

Another change worth noting is the clarification of the responsibilities of the data processor and his relationship with the controller. Under the GDPR, data processors

[65] Directive 95/46/CE: "Member States shall provide that the controller […] must notify the supervisory authority […] before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes"
[66] Directive 95/46/CE, Article 20: "Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official […]"
[67] Considering Article 35§3 of the GDPR, it is particularly the case regarding "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person", "processing on a large scale of special categories of data referred to in Article 9§1, or of personal data relating to criminal convictions and offences referred to in Article 10" and "systematic monitoring of a publicly accessible area on a large scale"
[68] GDPR, Article 36
[69] GDPR, Article 58§2
[70] GDPR, Article 33
[71] GDPR, Article 37§1

can no longer hide behind their status to avoid any responsibility[72]. They must actively participate in ensuring that the data processing carried out is compliant[73]. As was the case under the 1995 Directive[74], the relationship between the controller and the processor must be clarified by means of a legal act, but the GDPR is much more precise and demanding regarding the content of this act[75]. Similarly, the processor must report any data breach to the controller[76].

It should also be noted that data controllers may not use the services of a processor if the latter is unable to demonstrate that his activities comply with the GDPR[77]. The uncertainties that could have arisen when reading the 1995 Directive regarding the relationship between data controllers and processors have now been considerably reduced by the level of detail proposed in the text (level of detail which, as we will see, steers towards a vaguer nature in the UK data protection legal framework). Nevertheless, the practice of those involved in data processing and the guidelines developed by the supervisory authorities and the courts will all have to crystallize the various possible interpretations of the GDPR's provisions.

Let us this time delve into the ramifications of the strengthening of the prerogatives of the supervisory authorities:

As a symbol of the increasing power of the supervisory authorities, the amount of administrative penalties that can be imposed in the event of a breach of the GDPR is out of all proportion to what was provided for in the 1995 Directive. The latter was, moreover, very vague on this subject and left a great deal of room for manoeuvre to the Member States[78]. Under the GDPR, the supervisory authorities can now impose

[72] The data processor must, for example, cooperate with the controlling authority (GPDR, Article 31) and ensure the security of processing (GDPR, Article 32)
[73] GDPR, Article 28
[74] Directive 95/46/CE, Article 17§3
[75] GDPR, Article 28§3
[76] GDPR, Article 33
[77] GDPR, Article 28§1
[78] Directive 95/46/CE, Article 24: "The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive ."

fines of up to €20,000,000 or 4% of a company's worldwide annual turnover[79], whichever is highest, for the most serious breaches[80]. This level of penalty brings personal data protection law closer to competition law, where the European Commission is empowered to impose fines of a similar order of magnitude[81].

In conclusion of this second part, the GDPR, in addition to its enhanced power to impose penalties, is fully in line with Directive 95/46/EC. The other powers conferred on the supervisory authorities are reaffirmed, such as the powers of investigation, intervention and the ability to take legal action[82]. However, Article 58 of the GDPR is more specific about the scope of these powers. It gives the supervisory authorities a full range of powers, from a simple warning about a possible breach of the text[83] to the administrative fine described above.

It should also be noted that with the GDPR, the supervisory authorities are now responsible for checking certifications[84]. While these mechanisms demonstrate a certain "beginning of compliance", they do not constitute proof of compliance with the GDPR for the certified body[85]. For example, the supervisory authority is perfectly capable of withdrawing certification in the event of a breach of data protection legislation[86]. The GDPR also provides for the possibility of setting up a kind of decentralised certification system. It is thus possible for organisations to obtain certification from a supervisory authority in order to become certification bodies themselves[87]. This does not call into question the final role of the supervisory authority, which can withdraw the certification granted to a certifying body at any time as well as ask such a body to withdraw a certification granted to a company or actor that has been certified[88]. The system therefore enables national supervisory

[79] GDPR, Article 83§4: it is the highest amount out of the two which is retained
[80] GDPR, Article 83§5 and 6.
[81] See Articles 14 and 15 of Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings.
[82] Directive 95/46/CE, Article 28§3
[83] GDPR, Article 58§2
[84] GDPR, Article 42§5
[85] GDPR, Article 42§4
[86] GDPR, Article 58§2
[87] GDPR, Article 43
[88] GDPR, Article 58§2

authorities to rely on the additional support of certification bodies without being deprived of this task. This has and probably will further result in valuable financial and human gains, enabling the supervisory authorities to devote themselves to other tasks under the GDPR.

Part III: Comparison and analysis

Introductory remarks:

Initially launched in September 2021 under the title "Data, a new direction", the consultation published by the UK Government's Department for Digital, Culture, Media and Sport (DCMS), on its plans to reform data protection legislation and introduce the DPDI2 bill, took another step forward with its final response on the 17th of June 2022. Seen by some as a real "post-Brexit reward"[89], then-Digital Secretary Nadine Dorries and Minister of State for Media Julia Lopez welcomed this new progressive reform, aimed at ensuring that the UK can, in their words, "unlock the power of data to grow the economy and improve society" and emancipate itself from the "lack of clarity" and "cumbersome nature" of European legislation[90].

Describing this reform as an evolution rather than a revolution[91], the UK Government has outlined its main thrusts, while taking care to address the main areas of concern. However, a number of important points have not been addressed by this reform and remain unclear, raising questions and concerns which we will come to in this part III.

With a view to give data subjects control over their personal data outside the European Union, the DCMS proposed 30 headings divided into five main areas which were discussed and debated, amongst other issues of concern, in the Second Reading of the DPDI2 bill on Monday the 17th of April 2023, in the House of Commons. Those areas include reducing burdens on businesses, protecting consumers against nuisance calls and unnecessary cookies, modernising the powers of the Information Commissioner's Office (ICO), enabling innovative use of data and strengthening international trade.

In this first section, we will be highlighting and detailing those 5 main areas of change as presented and detailed by both the bill itself and the comments made by Government ministers, supporting said bill in debates and public statements. In our

[89] Clark, L. (2022), *Nadine Dorries promotes "Brexit rewards" of proposed UK data protection law*, The Register, 5th September.
[90] Montebello, L. (2022), *Dorries takes aim at GDPR with fresh data laws*, City A.M, 16th June

second section, we will confront those changes and promises made by the majority to both our and opposition MPs' concerns, all the while comparing them with EU GDPR provisions.

I. The DPDI2 Bill, promises of simplification and UK-centralisation

a. Lesser burdens on businesses through an ease of compliance

With regards to reducing burdens on businesses, specifically SMEs, the DCMS proposed that requirements such as the appointment of Data Protection Officers[92] (DPO), the creation of Data Privacy Impact Assessments[93] and Register of Processing Activities[94] would be removed and replaced by new obligations, as part of a "privacy management programme". So, for example, instead of a DPO, organisations will have to appoint a senior person responsible for data protection compliance.

As a result, members of the majority ensured that the same high standards of data protection would be maintained, but would concede greater flexibility to organisations in determining how they comply with them. According to Julia Lopez, the DPDI2 bill entails the most significant changes, regarding:

- Legitimate interest, which the European Commission defines as the legal grounds for processing data which is "not necessarily justified by a legal obligation or carried out to execute the terms of a contract with an individual"[95]. Under the new bill, there would be a limited number of pre-defined processing activities for which an organisation can invoke legitimate interest[96] without having to carry out a balancing test (consideration of the scope of the impacts of a processing of data and whether those override the identified interests[97]). These limited treatments include crime prevention and protection.

[92] GDPR, Articles 37 to 39
[93] GDPR, Article 35
[94] GDPR, Article 30
[95] Regulation EU 2016/679 of the European Parliament and of the Council, 27 April 2016, Recital 47
[96] DPDI2, Clause 5(4) subparagraph 9
[97] Information Commissioner's Office, 19 May 2023, UK GDPR guidance and resources / Lawful basis / A guide to lawful basis / lawful basis for processing / legitimate interests. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legitimate-interests/

- Anonymisation, which is not defined by the new data protection law but is contained in Recital 26 of the UK GDPR as "the way in which one turns personal data into anonymous information, so that it then falls outside the scope of data protection law"[98]. The DPDI2 bill indicates that an identification test would have to be conducted[99], based on whether anonymous data can be re-identified relative to the means available to the data controller to re-identify the data, as set out in the Council of Europe's Convention for the Protection of Personal Data (ETS No. 108). It is important to underline that the government wishes to avoid setting too strict a standard for anonymisation.

- Accountability, where a more flexible framework is envisaged, supported by privacy management programmes to reduce the time and resources that organisations (particularly SMEs) have to invest in compliance, and present a more proportionate approach to complying with the law. Organisations handling highly sensitive data will therefore, in theory, need to continue to implement a robust approach to accountability[100].

- Requests of access to personal data. Under the new DPDI2 bill, organisations will be able to refuse requests for access to information if the request is "vexatious or excessive"[101], replacing the current threshold of "manifestly unfounded or excessive", bringing it into line with the Freedom of Information regime[102].

[98] UK GDPR, Recital 26
[99] DPDI2, Article 84B (2 and 4)
[100] DPDI 2, clauses 12 (General obligations), 13 (Removal of requirement for representatives for controllers or processors outside the U.K.), 15 (Duty to keep records), 17 (Assessment of high-risk processing) and 18 (Consulting the Commissioner prior to processing)
[101] DPDI 2, clauses 7 and 8 (Vexatious or excessive requests and time limits for responding)
[102] Information Commissioner's Office (2017), *The Guide to Freedom of Information*, p.8

b. Protection of consumers

While the consultation mainly focused on possible changes to the UK GDPR and the Data Protection Act 2018, the DCMS also consulted on possible changes to the Privacy and Electronic Communications Regulations 2003 (so-called PECR Regulations 2003). The new reforms make a significant change to cookie consent[103], for they remove the requirement to display a cookie banner and allow cookies to be placed on a user's device without consent, and for a small number of non-intrusive purposes. However, members of the majority have insisted that websites will have to give users clear information on how to opt out (In Damian Collins' words, Conservative MP, "it is a question of having trusted systems for how data can be gathered, and giving users the right to opt out of such data systems more easily") [104].

Furthermore, in the future, the government is clearly indicating its intention to move to an opt-out consent model for cookies placed by websites, which has been supported by some members of the opposition (Lucy Powell, Labour/Co-op MP: "nobody likes nuisance calls or constant cookie banners, and the moves to reduce or remove them are welcome")[105]. This new opt-out model will reduce the need for users to click on consent banners on every website they visit.

However, non-commercial organisations would be able to rely on the flexible opt-in rule for sending commercial prospecting by e-mail. Nonetheless, the Sunak government has ensured that appropriate safeguards will be in place to protect individuals who no longer wish to receive advertising communications.

Organisations that fail to comply with the PECR rules will face fines equivalent to those under the UK GDPR[106], set at the current maximum of £500,000 for breaches of the PECR. Fines will increase from this maximum and will be aligned with the current UK GDPR penalties of up to 4% of worldwide turnover or £17.5 million, whichever is greater.

[103] DPDI2, clause 79 (Cookies and similar technologies)
[104] Damian Collins : Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons
[105] Lucy Powell: Ibidem.
[106] DPDI2, clause 86 (enforcement powers)

c. Modernising the ICO’s powers.

The ICO reforms were among the DCMS's most controversial proposals. In particular, concerns were raised that the reforms would undermine the independence of the ICO, which members of the majority were quick to dismiss. Although the government is introducing new obligations for the ICO as well as a new governance structure, it will not, according to the majority, go ahead with all of the projects originally planned.

According to the DCMS announcement, the ICO will be modernised with a chairman, chief executive and board of directors to ensure that its role as an internationally renowned controller continues. The change will introduce a broader set of skills to support robust decision-making and broaden the legal responsibility underpinning the ICO's work, which currently falls solely within the Information Commissioner's role.

It will now be mandatory for an individual to resolve their complaint with the data controller before referring the matter to the ICO, which should reduce the number of complaints made to the controller[107].

On paper, the Bill sets out strategic priorities emphasising the importance of the controller ensuring that data rights are respected and encouraging responsible use of data[108]. In addition, the reform gives the ICO new ways to develop statutory codes and guidance, sharing best practice for organisations that use, share or store sensitive data.

The ICO will be required to establish a panel of experts in the relevant fields when developing each statutory guidance. The Secretary of State will also be required to approve the ICO's statutory codes and guidance before they are laid before Parliament[109].

[107] DPDI2, clause 14 (Senior Responsible Individual)
[108] DPDI2, clauses 27 (Duties of the Commissioner in carrying out functions) and 28 (Strategic priorities)
[109] DPDI2, clause 30 (Codes of practice: panels and impact assessments)

d. Innovative utilisation of data

The DPDI2 Bill provides, as titled in its clause 2, a new statutory definition of "scientific research" and "statistical purposes"[110]. In a bid to strengthen the UK as a scientific superpower, the government sought to simplify and clarify the legal requirements for research to enable scientists to use data for innovation and scientific and technical development. Based on recital 159 of the UK GDPR, the changes are, on paper, unlikely to be substantial, however they raised concerns on behalf of the opposition which we shall come to.

The new definition seems to clarify and simplify the use of the data subject's consent to collect or use data and the subsequent processing for research purposes in general. Furthermore, it exempts data used in research from the requirement to provide a privacy notice where contacting individuals would require a disproportionate effort[111]. All in all, it is an approach which benefits the controller processing data collected for scientific research purposes.

Noteworthily, the government has not provided a new legal basis for research, for it was clear from public comments that the existing framework under Article 6 of the UK GDPR was sufficient[112].

[110] DPDI2, clause 2 (Definition of research and statistical purposes)
[111] DPDI2, clause 9 (Information to be provided to data subjects)
[112] Information Commissioner's Office, 21 February 2023, Corporate Information / Accessing UKHSA protected data / Approval standards and guidelines: lawful processing (UK GDPR)

e. Strengthening international trade

It has become clear that the highlighted objectives of the majority, through the DPDI2 bill, have been to stay committed to maintaining "high standards" of data protection and pursuing the free flow of personal data between like-minded countries. The UK Government noted the importance of removing barriers to cross-border data flows[113], including taking forward an ambitious programme of adequacy assessments. Indeed, Julia Lopez advanced that "the CBPR (Cross-Border Privacy Rules) system is one of the few existing operational mechanisms that, by design, aims to facilitate data flows on a global scale".

For example, the UK government is planning a risk-based approach to adequacy. Indeed, when assessing the granting of adequacy status to a third country, the government will not be required to review adequacy every four years[114]. Instead, there will be ongoing monitoring. In this way, exporters will be able to act pragmatically and proportionately where they use an alternative transfer mechanism. However, organisations will not be able to create or identify their own transfer mechanism. Instead, the UK Secretary of State will have a new power to recognise alternative transfer mechanisms as a form of security for the future[115].

The data reforms will support the UK Government's ambitions to enter into new data partnerships with major economies and improve international data transfers on which a number of technologies, such as GPS navigation, smart home technology and content streaming services, depend[116].

Vivienne Artz, Senior Data Strategy & Privacy Policy Adviser at the Centre for Information Policy Leadership, views the government's more flexible approach to

[113] Julia Lopez : Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons
[114] DPDI2, Article 45C
[115] Department for Digital, Culture, Media and Sport (2022), Consultation outcome, *Data: a new direction response to consultation*, A power to create alternative transfer mechanisms (questions 3.3.7, 3.3.8), 23rd of June
[116] Department for Digital Culture, Media and Sport (2022), Policy paper: UK Digital Strategy, 4th of October

data transfers as "a necessity, not a luxury in the increasing, increasingly digitalized and data driven economy"[117]. The government continues to work closely with international partners on data adequacy agreements with priority countries, such as the US, Australia, the Republic of Korea, Singapore, the Dubai International Financial Centre, Colombia, India, Brazil, Kenya and Indonesia[118].

However, the Government does not intend to exempt transfers from a third country to the UK, and then back to the third country, from the rules on international data transfers in the UK GDPR[119]. Nor does it intend to adopt provisions allowing a more flexible approach to exemptions for international data transfers.

Regarding concerns about data flows and the UK's adequacy with the European Union, the UK government insisted in its final response on the possibility and rationale of maintaining adequacy between the UK and the European Union when designing UK data protection legislation. In Julia Lopez's own words, "We are currently adequate, and we believe that we will maintain adequacy following the enactment of the Bill"[120]. Paul Scully, Parliamentary Under-Secretary of State for Science, Innovation and Technology stated that "it is important to note that the EU does not require exactly the same rules to be in place to be adequate". As a result, the majority believes that if the reform of the UK's personal data legislation is compatible with European Union adequacy rules, the continued flow of personal data from Europe will be possible[121].

[117] Artz, V., McCormack, P. (2023), Episode 21: Data Without Borders: Navigating Rights, Regulation, and Sovereignty, Privitar

[118] Department for Digital, Culture, Media and Sport (2021), Guidance: International data transfers: building trust, delivering growth and firing up innovation, 26th of August

[119] DPDI2, Schedule 7 (Transfers of personal data to third countries etc: consequential and transitional provision), clause 21

[120] Julia Lopez : Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons

[121] Paul Scully : Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons

II. Difference in provisions between the EU GDPR and UK DPDI2 bill – a negative impact for ease of compliance

a. Information relating to an identifiable living individual

The definition of personal data, as per section 3(2) and 3(3) of the UK Data Protection Act 2018, is currently laid out as "any information relating to an identified or identifiable living individual […] where a person is identifiable either directly or indirectly". However, clause 1(2) of the DPDI2 bill seeks to modify this definition allowing, in our view, for broader data processing with laxer protections.

Indeed, its qualification of personal data includes the condition in which it may only be qualified as such relative to either the "reasonable means" of the controller or processors "at the time of the processing" , or where the controller ought to reasonably know that "another person […] is likely to obtain the information as a result of the processing" and that "the living individual is likely to be identifiable by that person by reasonable means at the time of the processing" .

As such, the standard it establishes contains an exogenous element which narrows the range of information/data covered by the scope of data protection rules. Under the DPDI2 bill, information only qualifies as personal data when the data controller or processor can fairly identify the subject at the time of processing or when they have a good belief that "another person" can do so. By extension, this directly concedes more authority to data controllers, for the crux of the definition of personal data is no longer the personal nature of the information itself, but rather the context and, more importantly, the extent of the processing powers of the handlers themselves. By hacking at the current scope of UK data protection laws (which, as we ought to remind for context, are directly calqued on the EU GDPR), the new scope has also raised concerns, notably on behalf of Dr. Chris Pounder, Director of the Amberhawk consultancy group, about the impact the new legislation may have on facial recognition and CCTV systems.

The new bill would permit widespread facial recognition operations throughout the UK for individuals who are not on watchlists, both through video but also online surveillance, with personal photos and public information scraped from the internet to be processed in unprecedented quantities, under the new legal guise that the processor would be unable to recognise the individuals whose data is processed.

The principles of data protection legislation, relative to EU principles, are therefore at a huge different since they substitute a clear and objective definition of personal data for a subjective one, basing individual rights on an organisation's processing capacity.

b. Lawfulness of processing

The lawful nature of processing is constrained, under article 6 of the UK GDPR, by 6 different conditions, including the necessity for it to be "for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data". However, clause 5 of the DPDI2 bill seeks to modify this notion allowing again, in our view, for broader data processing with laxer protections.

Indeed, the DPDI2 bill amends the current article 6 by introducing the notion of "recognised legitimate interests", in which the balancing test, as defined previously as the consideration of the scope of the impacts of a processing of data and whether those override the identified interests, would no longer be required.

This yet again hacks at the scope of the UK GDPR under which personal data fell, and offers larger quantities of data, no longer deemed personal, to be processed by both public and private entities. Furthermore, under section 4(7) of Clause 5, the Secretary of State would have the power to determine said recognised legitimate interests by "having regard to, among other things, the interests and fundamental rights and freedoms of data subjects which require protection of personal data"[122].

[122] DPDI2 bill, Clause 5, section 4(7)

Notably, annex 1 of the DPDI2 bill recognises legitimate interests in data processing without a balancing test for matters of "natural and public security, defence, emergencies, crime and democratic engagement" , which raises some concerns which we shall come to later in our analysis.

Furthermore, section 4(9) of clause 5 of the DPDI2 bill states a series of examples of "types of processing that may be processing that is necessary for the purposes of a legitimate interest"[123], including: intra-group transmission of personal data; processing that is necessary for marketing and for purposes of ensuring the security of network and information systems. As opposed to the European framework for data protection, this provision allows businesses to use the public's personal data without necessarily obtaining consent, effectively edging the consideration of the former closer to products as opposed to individuals with rights to protection and control over their own data.

Practically, this would translate to the public losing the benefits of the UK GDPR regarding the mitigation of unwanted spam emails/calls and, more seriously, disproportionately impact individuals who suffer from disproportionate data collection (i.e. people in the welfare system, criminal justice systems or pensioners)[124].

In line with our first section of the present Part III, members of the majority insisted the new bill relied on the intention to concede greater flexibility to organisations in determining how to comply with data privacy laws, all the while maintaining high standards for data protection. However, by debilitating both the definition of the notion of personal data and broadening the purposes for its processing, one could argue the majority has effectively conducted an assault on the foundations of privacy laws both within and outside of the UK, distancing themselves from Convention 108 and thwarting their own attempts at conserving adequacy with the EU.

[123] DPDI2 bill, clause 5 section 4(9)

[124] Big Brother Watch, 'Poverty Panopticon: The hidden algorithms shaping Britain's welfare state' (20 July 2021) https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf

c. Purpose limitation

The purpose limitation principle, set out in article 5 of the UK GDPR, can be defined as "a requirement that personal data be collected for specified, explicit and legitimate purposes, and not be further processed in a manner that is incompatible with those purposes"[125].

Article 5 can already be constricted by law compared to the EU GDPR, ""when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard national security, defence, public security, crime prevention, among other purposes.

However, clause 6 of the DPDI2 bill further restricts the notion of purpose limitation by introducing Article 8A to the UK GDPR, which would permit the Secretary of State to pre-emptively exempt certain data from the purpose limitation principle as long as the processing meets the conditions laid out under (new) Annex 2 of the UK GDPR.

One of two main concerns here would be that this new provision would concede even more Henry the VIIIth powers to the Secretary of State, the latter being granted, under clause 6, the ability to amend the conditions set out in annex 2 of the UK GDPR by "adding or varying provisions" or "omitting provisions added by regulations"[126] by using the "affirmative resolution procedure"[127].

Furthermore, such an amendment would be lawfully operated as long as the Secretary of State considers "that processing in that case is necessary to safeguard an objective listed in Article 23(1)(c) to (j)" of the UK GDPR.

Lastly, this reformulation of the derogations to articles 5 and 23 of the UK GDPR is oblivious to the current possible exemptions, which ought to "respect the essence of

[125] UK GDPR, article 5(1)(b)
[126] DPDI2 bill, Clause 6, section 5
[127] DPDI2 bill, Clause 6, section 8

the fundamental rights and freedoms" and be a "proportionate measure in democratic society"[128].

As similarly argued in our previous subsection, we consider this once again an attack on the foundations of privacy laws in the UK, specifically the removal of the explicit requirement of proportionality tests, which pave the way to the normalisation of processing and unconsented use of the public's data at the hands of an overtly-powerful Secretary of State.

d. Vexatious or excessive requests by data subjects

Article 12 of the UK GDPR provides that "the controller shall take appropriate measures to provide any information […] and any communication […] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form". This 2018 provision seems to naturally engrain itself as a continuation of the principle of accountability[129], for it is only natural for one to have the right to access and view one's data, otherwise one could not fully enjoy one's data rights.

Nevertheless, it is also natural, in cases in which data subjects' rights requests are unfounded or excessive, for the controller to refuse such an access. The conditions for such refusals are, in turn, encapsulated in paragraph 5 of article 12, which states that "where requests from a data subject are manifestly unfound or excessive, because of their repetitive character, the controller may either charge a reasonable fee […] or refuse to act on the request"[130].

However, clause 7 of the DPDI 2 bill diminishes this right by qualifying the nature of the requests which may be refused as "vexatious" or "excessive", for which no definition is provided for the former.

[128] UK GDPR, article 23(1)
[129] Article 29 Working Party, Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010 (WP 173). For more on accountability and compliance, see infra Section 7, Part B.
[130] UK GDPR, article 12(5)

Furthermore, the determination of the "vexatious" or "excessive" nature of the request would have to be made whilst "having regard to the circumstances of the request" under section 10[131], which under the non-exhaustive list provided includes "the resources available to the recipient"[132].

This appears to us as a flawed basis on which to provide whether an individual's request of access to their data is vexatious or excessive.

Indeed, Darren Jones, Labour MP for Bristol North West, stated during the second reading of the DPDI2 bill in the house of commons that "reducing unnecessary compliance burdens on business is of course welcome, but the Government seem to have forgotten that data protection law is based on a foundation of protecting the consumer, not being helpful to business"[133].

Clause 7 of the DPDI2 bill finds itself directly in line with the concerns of the member of the opposition Darren Jones for it creates a disobliging incentive for both public and private entities to underresource data record management. Combined with the possibility for the controller to charge a fee for any subject access request, this creates a disbalance in the power dynamic between consumers and businesses that reporter Vincent Manancourt warned against in November of 2022: "Human rights should not be diluted for the purpose of business interest. However, given the consensus from civil society that the DPDI2 Bill is "even worse" than its previous iteration, it is clear that this is what the current proposals will do"[134].

[131] DPDI 2 bill, section 10 – 204A (1)
[132] Ibidem, paragraph (c)
[133] Darren Jones, Labour MP, Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons
[134] Manancourt, V. (2022) ''We were taken for fools": MEPs fume at UK data protection snub', 7 November https://www.politico.eu/article/we-were-taken-for-fools-meps-fume-at-uk-data-protectionsnub/

e. Automated decision-making

Under article 22 of the UK GDPR, data subjects have a recognised right "not to be subject to a decision based solely on automated processing, including profiling, which affects" or "produces legal effects concerning him or her"[135], unless there is a legal basis to do so (i.e. explicit consent of the data subject (c), where such an undertaking is required by law (b) and when it is necessary to enter into a contract with a data controller (a))[136]. Recital 71 of the EU GDPR further underlines the necessity of having exhaustive conditions for derogations to article 22(1)[137].

However, clause 11 of the DPDI 2 Bill replaces article 22 with section 4A containing article 22A-D, redefining automated decisions. As opposed to broadly prohibiting automatic decision-making (thereinafter, ADM) with certain exemptions, article 22A-D widens the circumstances in which ADM may be exclusively used with only very little restrictions:

Firstly, article 22C(1) (*safeguards for ADM*) only requires the controller to "ensure that safeguards […] are in place" and that they "include measures which provide the data subject with information about the automated decision […] and enable them to make representations […], contest […] and obtain human intervention with regard to the decision". As it stands, current legislation requires notification to an individual which has been subjected to ADM, effectively marking this duty as a proactive obligation, as opposed to its shaping into a reactive responsibility under the new clause. It is made clear in paragraph 177 of the DPDI 2 explanatory notes that newly permitted automated decisions would not be subject to the current legal safeguard of notification: "where appropriate, this may include notifying data subjects after such a decision has been taken" (emphasis on the "where appropriate" and "may").

This trend of *opacification* and dilution of the elementary safeguards of ADM should come off as alarming to one, for data subjects might not even be aware that they are

[135] UK GDPR, article 22(1)
[136] Ibidem, article 22(2)
[137] UK GDPR, recital 71(2)

being subjected to the former and therefore unable to adequately exercise their legal rights if it is conducted in secret.

Indeed, Manchester Central Labour MP Lucy Powell expressed her own concerns with regards to ADM during the second reading of the DPDI2 bill in the House of Commons: "(under the new bill) data protection impact assessments will no longer be needed, and protections against automated decision making are being weakened"[138], followed by Glasgow North West SNP MP Carol Monaghan: "clause 11, if implemented, would mean that solely automated decision making is permitted in a wider range of contexts"[139].

Secondly, article 22B (*restrictions on ADM*) states that "a significant decision based on special categories of personal data", which are provided for in article 9(1) of the UK GDPR, "may not be taken based solely on automated processing unless the decision is based entirely on processing of personal data to which the data subject has given explicit consent" or if "the decision is required by law" or if "the decision is necessary for entering into, or performing a contract between the data subject and a controller" or where "point (g) of Article 9(2)[140] applies".

Point (g) of Article 9(2) of the UK GDPR concerns processing "necessary for reasons of substantial public interest", which is a legal basis which may solely be used as a substance to process *special* categories of data. As such, article 22(B) exempts decisions authorised by law in any category other than special categories mentioned in article 9(2)(g), as opposed to the scope of the UK GDPR which encompasses all data categories.

Put in simpler terms, the scope of the current legislation encompassing both *special* and *non-special* categories of data would be hacked to solely encompass special categories. One could argue that this is cause for concern, for when used in ADM, personal data that does not fall under a special category can serve as a proxy for protected qualities listed in article 9(1) UK GDPR. Data which has been given consent

[138] Lucy Powell, Labour MP, Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons
[139] Carol Monaghan, SNP MP, Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons
[140] Article 9(2)(g) of the UK GDPR

to be processed regarding somebody's name, address/postcode or profession can act as a proxy for their sex or ethnicity when processed by an algorithm for example.

In its assessment for the DPDI 2 Bill, the Public Sector Equality Duty acknowledged this issue, which notably appeared when an AI grading system predicted grades for university entrance exams, disproportionately lowering the results of disadvantaged students: "Though precautions were taken to prevent bias based on protected characteristics, the profiles of those attending different schools inevitably led to outcomes being different based on their protected characteristics, including race and sex"[141].

This again embeds itself in the trend of watering and narrowing down the scope of data protection laws; we find it crucial for ADM to remain subject to heavy restrictions and few exemptions, as opposed to few restrictions and many exemptions which the DPDI 2 bill seeks to introduce. NGOs such as Algorithm Watch have warned against the extended use of ADM due to the biased nature of algorithms[142], which tend to operate on qualitative input, privileging certain categories of data over others in ways different from the intended function of the algorithm[143]. As article 22A-D will increase the number of automated decisions by algorithms, there can only and naturally be an increase in its negative effects.

Stephanie Peacock, Labour MP for Barnsley East, voiced her concern on the amending of article 22 of the UK GDPR in the second reading of the DPDI 2 bill in the House of Commons, stating that many legal cases "explicitly relied on current legislation in the form of article 22 of the UK GDPR, and a clear understanding of what constitutes meaningful human involvement. Without providing clear boundaries for defining significant decisions and meaningful human involvement, this Bill therefore risks removing the exact rights that won this case and creating an environment where vital safeguards, such as the right to contest automated decisions

[141] Public Sector Equality Duty assessment for Data Protection and Digital Information (No.2) Bill - DSIT, 8th March 2023: https://www.gov.uk/government/publications/data-protection-and-digital-informationbill-impact-assessments/public-sector-equality-duty-assessment-for-data-protection-and-digitalinformation-no2-bill

[142] Algorithm Watch (2023), '*The ADM Manifesto'* https://algorithmwatch.org/en/the-adm-manifesto/

[143] Friedman, B., Nissenbaum, H. (1996), "Bias in Computer Systems", *ACM Transactions on Information Systems*, Association for Computing Machinery Digital Library.

and request human intervention, could easily become exempt from applying at the whim of the Secretary of State. This must be resolved, and the public must be reassured that they will not be denied a job, mortgage or visa by an algorithm without a method of redress."[144]

Thirdly, article 22D of the DPDI2 bill provides entire power over how the ADM regulatory framework operates to the Secretary of State, by means of secondary legislation.

Paragraphs 1 to 4 state that the Secretary of State may, using regulations: provide that "for the purposes of article 22A(1)[145], there is, or is not, to be taken to be meaningful human involvement in the taking of a decision in cases described in the regulations"[146]; provide that "a description of a decision is, or is not, to be taken to have a similarly significant effect for the data subject"[147]; make further provision "about the safeguards required under article 22C(1), including provision about what is, or is not, to be taken to satisfy a requirement under article 22C(1) or (2)"[148].

By amending article 22 of the UK GDPR to include such an exceptional scope for political arbitration, the DPDI 2 bill, through concession of powers to the Secretary of State to bypass the new regulatory framework of ADM, effectively undermines the very purpose of a legislative framework for data regulation.

[144]Stephanie Peacock, Labour MP, Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons

[145]DPDI2 bill, article 22A(1): "For the purposes of articles 22B and 22C – a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision (a), and a decision is a significant decision, in relation to a data subject, if it produces a legal effect for the data subject or it has a similarly significant effect for the data subject (b)".

[146] DPDI2 bill, article 22D paragraph 1

[147] Ibidem, paragraph 2

[148] Ibidem, paragraph 4

f. National security exemption

The Data Protection Act of 2018 provides, in its Part 3, the rights of individuals to accession, rectification, erasure or restriction of their personal data. The notion of restriction refers to the right of a controller to derogate from his obligation to inform individuals about personal data breaches, "where it is necessary and proportionate to protect national security". To enjoy this right, controllers must demand a Minister of the Crown to issue a certificate relating to the national security provision they wish to apply for, act which is provided for in section 27 of the DPA 2018[149].

Clause 24(7) of the DPDI 2 bill changes the effects and the scope of these national security certificates, which would generally exempt law enforcement from a plethora of the most basic obligations under the DPA 2018. The most significant changes include the exemption of sensitive processing[150]; the exemption of the purpose limitation principle[151]; the exemption from rectifying inaccurate and outdated personal data[152] and the exemption from withholding and storing personal data longer than what the original purpose of processing would require for[153].

These new changes yet again engrain themselves in the trend of hacking at the scope of applicable data protection law by including "most of the data protection principles, rights of data subjects, obligations on competent authorities and processors, and various enforcement provisions"[154] in the list of exemptible material for data controllers. Furthermore, a certificate may be specific or general under the DPA section 79(2); the DPDI would amend this provision to solely make them general.

Paired with the fact that an issuance of a certificate is considered "conclusive evidence" for a national security exemption, and that national security certificates are exempt from proportionality tests, clause 24 essentially grants intelligence services and law enforcement a ticket to act above the law and disregard the most fundamental

[149] DPA 2018, section 27: National Security - certificate
[150] Amendment of the DPA 2018 section 35(3) by the DPDI2 bill's article 78A(3)(b)
[151] DPDI2 bill article 78A(2)(a)
[152] Ibidem
[153] DPDI2 bill clause 79(2)
[154] Data Protection And Digital Information bill - Explanatory Notes, 8th March 2023: https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf 23

data protection principles. This further undermines data regulation and plunges us deeper into techno-authoritarianism in which data regarding genetics, biometrics, race, political opinions, health, sexual orientation, religious and spiritual beliefs can be in secrecy and for unjustified purposes.

g. The ICO's independence

The Information Commissioner's Office's role, according to the UK's official government website, is to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"[155]. Additionally, it is responsible for monitoring government data activities.

However, clause 27 of the DPDI2 bill introduces article 120B, which places "the desirability of promoting innovation and competition" as the prism from which the ICO should carry out its functions. This characterises the public's data as a resource ripe for exploitation, rather than private information that warrants protection. Imposing business interests upon the functions of the ICO undermines its core purpose of regulating data protection in the UK.

We are yet again confronted with the privacy vs security dilemma in article 120B, for it would require the ICO to consider the importance of the "prevention, investigation, detection and prosecution of criminal offences" and "the need to safeguard public security and national security"[156]. On top of conceding "creep powers" to the highest data-regulation enforcing power of the country, it increases the risks of politicising this non-departmental public impartial body.

Furthermore, clause 28 introduces articles 120E and 120F, empowering the Secretary of State to guide the ICO with strategic priorities "which he must have regard to when

[155] Information Commissioner's Office, GOV.UK: https://www.gov.uk/government/organisations/information-commissioner-s-office#:~:text=The%20Information%20Commissioner's%20Office%20(ICO,for%20Science%2C%20Innovation%20and%20Technology.

[156] DPDI2 bill, article 120B

carrying out functions under the data protection legislation"[157]. The possibility for government to push their interests upon the ICO is likely to endager his impartial application of the law.

[157] DPDI2 bill, article 120E

Part 4: Considerations on Big Data as a Pandora's Box towards digital authoritarianism

The massive collection of data and its processing by algorithms, made possible by digital technologies, seems to be leading to the emergence of new types of knowledge, whose objectivity seems absolute, on the pretext that it derives directly from the automatic calculation carried out on raw data recorded by computational systems. However, the profiling thus established on the basis of statistical correlations, while suspending any kind of subjective intervention (such lack of subjective intervention and lack of information of the latter to the data subject with regards to ADM being subject to heavy restrictions and few exceptions under the UK GDPR and DPA, as opposed to the DPDI2 bill), remains unavailable and imperceptible to the individuals to whom it is nevertheless applied. These measures make it possible to anticipate their behaviour, only insofar as they affect their desires and wills (and destroy their singularity), by constantly reconfiguring their informational environments in real time. Far from producing knowledge about the social world that subjects could appropriate, think about and question collectively, this algorithmic "rationality" therefore constitutes an unprecedented mode of government, based on a new type of dogmatisation, which pre-empts any possibility of criticism, discussion or testing, by imposing itself in the name of innovation and security.

To serve as an example, neither in China nor in other Asian states such as South Korea, Hong Kong, Singapore, Taiwan or Japan is there a critical awareness of digital surveillance or "Big Data", which we defined in section II of our Part 1.

In this era, the relationship that subjects have with their digital devices has changed the pace, time and intensity with which their users experience reality. This relationship intensifies the coercive use that algorithms can exert on humanity.

According to philosopher Byung-Chul Han, in his book Psychopolitics: Neoliberalism and the New Technologies of Power[158], we live in an age, neoliberalism, where its

[158] Han, B.C (2017), *Psychopolitics: Neoliberalism and the New Technologies of Power*, translated by Eric Butler, Verso Books, pp. 28-38

protagonist, the neoliberal subject, lives in an illusion of freedom, voluntarily surrendering not his skin, but his mind. According to Han, we are entering the age of digital Psychopolitics, or the moving from passive surveillance of society to its active management. As such, it is precipitating us into a major crisis of freedom, in which the latter itself is at stake. Big Data is, in this sense, a highly efficient psychopolitical instrument that makes it possible to achieve a comprehensive understanding of the dynamics of social communication[159].

In a nutshell, the Big Data device, results from a need to accumulate computer data. From scientific knowledge, to financial data, to the social network profiles we voluntarily hand over, they are a source of business and power. The dilemma that arises is whether this instrument could predict the behaviour of subjects, thereby discriminating against junk or low-scoring subjects, as Han points out in his article on the pandemic.

Indeed, data is a resource that concerns individuals. But once it has been aggregated, it is also a collective resource. Massive data is the major input for value creation in the connected world, such as advertising targeting and algorithm-based decision-making processes. The same is true of most processes that use data generated by the actions of every member of the community. To date, this resource has been cornered on derisory terms by the major Internet players.

Privacy laws regard data as an essentially individual matter, as we have noted in sub-section (g) of Section II Part 3. This is why they insist on requiring individuals to "consent" to the collection and use of their personal data. As long as the individual has consented, a company can do whatever it likes with the data it collects.

Imposing quid pro quos for the right to take advantage of the massive data produced by the community should be amongst the guiding principle of the laws governing digital companies. By recognising that data, once it has become massive (Big Data), is a collective resource, governments would give themselves the legitimacy to attach conditions to the processes by which the Web giants generate value from data captured

[159] Ibidem, p.11

from a population, most notably through automated decision making (Part 3, Section II sub-paragraph (e)).

Is it not legitimate for communities to have a right to transparency and information regarding the actions of companies that generate value from resources obtained by observing the interactions of individuals in said community?

It must be emphasised that recognising the status of mass data as a collective resource does not mean that the State has the right to monopolise the data of individuals in defiance of the guarantees protecting their privacy and dignity. Like common goods, such as the air and water that everyone uses, data is personal when it is linked to an individual. But when air and water or data become detached from the individual, they once again become part of the environment, a resource with implications for the community. It is only natural that legal frameworks such as the GDPR should govern not only the extent to which data is collected, but also stored and processed.

In the meantime, a laxer and more intrusive legal framework for data collection, such as the newly proposed DPDI2 bill, has ignited concerns about the potential for population and behavioural control, notably through the exploitation of big data.

The utilization of big data for influence over a population is not a far-fetched concept but rather a reality witnessed in various historical contexts. For instance, the Chinese government's social credit system serves as a prime example of how extensive data collection and analysis can be employed to monitor and control citizens' behaviour. By assigning social scores based on individuals' actions, associations, and online activities, the government can incentivize conformity and punish dissent. This system showcases how the exploitation of big data can result in a pervasive surveillance apparatus that regulates and shapes citizens' behaviour, eroding personal freedoms and fostering a climate of compliance.

The use of big data for behavioural influence indeed raises concerns about the manipulation of individuals' choices and decision-making processes by both public and private entities. The analysis of vast datasets allows for the identification of patterns, preferences, and biases, enabling the crafting of personalized messages and

interventions that steer individuals in desired directions, notably under the DPDI2 bill, which allows for ADM to be conducted, without the need to inform the data subject. A watered-down legal framework for data protection entails a heightened manipulation of behaviour which not only undermines individual autonomy but also poses a significant threat to democratic processes, as it distorts the marketplace of ideas. Furthermore, in the case of the DPDI2 bill, it allows for the Secretary of State to make use of Henry VIIIth powers to bypass the rights and obligations enshrined within the legal framework, by allowing law enforcement and intelligence agencies to aggregate and process sensitive biometric data for the purpose of crime prevention through population surveillance. Unlike the general prohibition on ADM involving certain categories of sensitive data for private entities, the Bill's ECHR memo states that "controllers processing for law enforcement […] will make it more possible for the police and others to use this technology. Currently the requirement to inform an individual whenever automated decision-making takes place limits operational usefulness"[160].

The potential for population control and behavioural manipulation through big data becomes indeed even more alarming when combined with surveillance tools. The integration of facial recognition technology, biometric data, and social media monitoring amplifies the ability of authoritarian regimes to monitor and track individuals in real-time. This comprehensive surveillance infrastructure further empowers governments to not only observe citizens' behaviour but also intervene and suppress dissent at a moment's notice. This last concern notably stems from the introduction of 15-minute cities in the UK, in which, under the new DPDI2 bill, would allow for the effective use of biometric tools to restrict freedom of movement between "zones" in the UK, under the guise of the necessity to control pollution levels. The chilling effect on freedom of movement and the erosion of privacy rights in such a scenario are substantial and must be taken seriously.

To mitigate these risks, it is crucial to establish and undeviate from robust safeguards and regulations that protect individuals' privacy and prevent the abuse of big data.

[160] Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum - 8th March 2023, para.19, p.9

Transparency and accountability should be at the core of any legal framework governing data collection and analysis. Citizens must have clear knowledge of what data is being collected, how it is being used, and the mechanisms in place to safeguard their privacy. Additionally, oversight mechanisms, such as independent regulatory bodies and judicial review, should be established to ensure that data collection practices adhere to legal and ethical standards. All the above-mentioned necessities are either scrapped or can be subject to derogation under the new DPDI2 bill, under the guise of innovative and competitive use of data, the necessity to limit vexatious requests, and national security.

Ethical considerations should also play a central role in the utilization of big data. Governments and organizations must adhere to ethical guidelines that prioritize individual autonomy, consent, and the prevention of harm. Responsible data governance should include principles such as data minimization, purpose limitation, and the right to opt-out or be forgotten. By upholding these ethical standards, the risks of population control and behavioural manipulation can be mitigated, and the potential for authoritarian exploitation of big data can be curtailed.

Conclusions

In conclusion, a laxer and more intrusive legal framework for data collection, exemplified by the DPDI2 bill, raises significant concerns about the potential for population surveillance and behavioural control and influence through the exploitation of big data.

By harnessing the power of advanced analytics and artificial intelligence, both public and private entities can gain unprecedented insights into individuals' behaviour, preferences, and vulnerabilities. This wealth of information enables them to create highly targeted publicity, manipulate public opinion, and influence electoral outcomes. By leveraging sophisticated algorithms and predictive models, such entities can exploit the vulnerabilities of human psychology and nudging techniques to control and influence behaviour.

Drawing on the insights of political philosophers and historical examples, we can understand the dangers associated with utilizing advanced analytics and artificial intelligence to manipulate and shape public behaviour. It is crucial to establish robust safeguards, promote transparency and accountability, and adhere to ethical principles to prevent the abuse of big data and preserve individual freedoms in the face of creeping population influence and the risk of authoritarian tendencies.

Bibliography:

Dură, Nicolae V (2019), *About the Freedom of Religion and the Laicity. Some Considerations on the Juridical and Philosophical Doctrine*, Bulletin of the Georgian National Academy of Sciences, Tbilisi.

Gajda, Amy (2022), *Seek and hide: the tangled history of the right to privacy*, Viking, New York.

Richardson, Megan (2017): The Right To Privacy: Origins And Influence Of A Nineteenth-Century Idea, Cambridge University Press, Cambridge.

United Nations, *Universal Declaration of Human Rights*, 1948.

Council of Europe, *European Convention on Human Rights*, 1950.

Case Law: Rubio Dosamantes v. Spain, 21/02/2017.

Council of Europe, *European Convention on Human Rights*, 1950.

Spanish Yearbook of International Law Online 1, 1, 197-238, sentence 197/1991, 17/10/1991.

Rolla, G. (2001), *The difficult balance between the right to information and the protection of dignity and private life. Brief considerations under the light of Italian experience*, In Law and Person, no. 44.

Fry, James P. & Sibley, Edgar H. (1976), *Evolution of Data-Base Management Systems*, ACM Computing Surveys, Volume 8, Issue 1.

Council of Europe's Ministerial Council (26/09/1973), resolution nº73, on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector.

Council of Europe's Ministerial Council (20/09/1974), resolution nº74, on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector.

Council of Europe (28/01/1981), *Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data*.

De Terwangne, C. (2011), *Internet Privacy and the Right to be Forgotten/Right to Oblivion*, Internet, Law and Politics Magazine.

Case Law : Ombudsman of the People v Attorney General, Constitutional appeal, STC 292/2000, ILDC 128 (ES 2000), 30th November 2000, Spain; Constitutional Court.

Case Law : Scarlet Extended SA v Sabam (24th November 2011) (C-70/10) EU:C:2011:771.

Case Law : Breyer v Germany (19th October 2016) (C-582/14) EU:C:2016:779.

Case Law: joined cases: Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärnter Landesregierung (C-594/12).

Godwin, M. (2003) *Cyber Rights: Defending Free Speech in the Digital Age*, MIT Press, London, 10.

Floridi, L (2014): The fourth revolution : *How the infosphere is reshaping human reality*. Oxford University Press, Oxford.

Vashist, A. (2021), Theory of Extraterritoriality of States and Jurisdiction in International Law, Legal Service India, E-Journal, Raffles University Neemrana.

Kramer X. , Rooij M. de, Lazic V. , Blauwhoff R. , Frohn L. (2012) *A European Framework for private international law : current gaps and future perspectives*, Directorate General for Internal Policies, Policy Department C : Citizen's rights and constitutional affair, European Union.

Brussel, J (2013) Definition of "*cyberspace*", Encyclopaedia Britannica.

Abbot, C (2012) Bridging the Gap – *Non-state Actors and the Challenges of Regulating New Technology*, Journal of Law and Society, Vol. 39.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Union, *Treaty of the European Union*, 1992.

European Union, *Treaty of the Functioning of the European Union*, 1992.

Swedish Data Act (SFS 1973:289) 11 of May, 1973.

German Federal Data Protection Act of 1977 : *Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act* - . BDSG).

French Law no. 78-17 of 6th of January 1978 on data processing, data files and individual liberties.

President Juncker's political guidelines presented during the opening speech of the plenary session of the European Parliament on 15 July 2014 in Strasbourg.

Case Law : Politi s.a.s. v Ministry for Finance of the Italian Republic (14/12/1971), Court of Justice of the European Communities, C-43/71.

European Union, *General Data Protection Regulation*, 2018.

French Law of the 06/01/1978 relative to data processing, data filing and individual liberties, modified.

Case Law: Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González (13/05/2014) case C-131/12 regarding the right to be forgotten.

Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings.

Clark, L. (2022), *Nadine Dorries promotes "Brexit rewards" of proposed UK data protection law*, The Register, 5th September.

Montebello, L. (2022), *Dorries takes aim at GDPR with fresh data laws*, City A.M, 16th June.

House of Commons, *Data Protection and Digital Innovation Bill 2*, 2023.

Information Commissioner's Office, official website.

Second Reading of the DPDI2 bill, Monday the 17th of April 2023, in the House of Commons.

Department for Digital, Culture, Media and Sport (2022), Consultation outcome, *Data: a new direction response to consultation*, A power to create alternative transfer mechanisms (questions 3.3.7, 3.3.8), 23rd of June.

Department for Digital Culture, Media and Sport (2022), Policy paper: UK Digital Strategy, 4th of October.

Artz, V., McCormack, P. (2023), Episode 21: Data Without Borders: Navigating Rights, Regulation, and Sovereignty, Privitar.

Department for Digital, Culture, Media and Sport (2021), Guidance: International data transfers: building trust, delivering growth and firing up innovation, 26th of August.

Big Brother Watch, 'Poverty Panopticon: The hidden algorithms shaping Britain's welfare state' (20 July 2021).

Working Party, Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010 (WP 173).

Manancourt, V. (2022) ''We were taken for fools": MEPs fume at UK data protection snub', 7 November.

Public Sector Equality Duty assessment for Data Protection and Digital Information (No.2) Bill - DSIT, 8th March 2023.

Algorithm Watch (2023), '*The ADM Manifesto'*.

Friedman, B., Nissenbaum, H. (1996), “Bias in Computer Systems”, *ACM Transactions on Information Systems*, Association for Computing Machinery Digital Library.

House of Commons, *Data Protection Act*, 2018.

[1] Han, B.C (2017), *Psychopolitics: Neoliberalism and the New Technologies of Power*, translated by Eric Butler, Verso Books.