---

**Article:**
Omotubora, A and Basu, S orcid.org/0000-0001-5863-854X (2020) Next Generation Privacy. Information & Communications Technology Law. ISSN 1360-0834

https://doi.org/10.1080/13600834.2020.1732055

---

# Next Generation Privacy

*Adekemi Omotubora
University of Lagos Nigeria (aomotubora@unilag.edu.ng)

**Subhajit Basu
University of Leeds UK (s.basu@leeds.ac.uk)

**Abstract**

In recent years, research within and outside the European Union (EU) has focused on the expanding scope of personal data. The analysis provided has primarily supported the conclusions that in time, personal data will become so ubiquitous that the EU data protection law would become meaningless, unreasonable, or even discredited and ignored. Notwithstanding these criticisms, EU law is promoted as the 'gold standard' for data protection laws and the law, including its definition of personal data, is being rapidly adopted by many non-EU countries. The objective of this article is to analyse the concept of personal data under EU law and to explore its continued relevance within a data protection framework that is rapidly globalised and in which technology is continuously evolving. The article argues that far from reflecting a universal notion of data protection, the EU law and particularly its definition of personal data reflects a perception of privacy that is peculiarly European. It further argues that recent developments in technology call for a re-examination of the concept of personal data and a more critical approach by countries with nascent data protection regimes. The article proposes the 'objective risk of contextual harm' as a new approach for formulating an alternative definition of personal data. It concludes that this approach better articulates the construction of data protection as a social good and a mechanism for (consumer) protection.

**Keywords** - privacy, data protection, personal data, identifiability, new technologies, contextual harm

## 1. Introduction

The EU's approach to data protection is repeatedly held up as the "gold standard" for data protection regulation. Its touted advantages include that it takes an omnibus approach to data protection, contains fundamental principles to govern data processing, takes a rights-based approach to the protection of data subjects, and establishes public regulatory bodies to administer the law and monitor compliance. However, the EU regime contains within it a potentially fatal flaw. The definition and interpretation of personal data create core concerns about the sustainability of data protection regimes, without the amendment, it is unlikely that the EU regime is capable of transitioning into an adaptive regime capable of operating in a global arena.

Under Article 4 of the General Data Protection Regulation (GDPR)[1] (which replaced the Data Protection Directive[2]), personal data is defined as

> *Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.*

In construing a similar provision under the Directive,[3] the Article 29 Working Party (WP29) made it clear that identification or identifiability, is the threshold criterion for determining whether data is personal.[4] According to the WP29, the words, "any information" contained in the Directive signals the willingness of the legislator to design a broad concept of personal data and calls for a wide interpretation.[5] The WP29 argued that all forms of information qualify as personal data unless the possibility of identification does not exist or is negligible.[6] In previous legislative guidance, personal data has been held to include factual identifiers such as a person's name, address, date of birth, and indirect identifiers such as phone numbers, profile data drawn from a combination of innocuous pieces of information,[7] and information relating to devices and objects such as IP addresses.[8] The web traffic surveillance tools, including cookies, and geolocation and traffic data also constitute personal data.[9] The WP29 further indicated that consideration must be given to state of the art in technology because the information which is currently unidentifiable may subsequently become identifiable due to technological development.[10] In effect, prospective or merely speculative data can be personal data. The significance of this interpretation lay in the fact that it is sufficiently broad to cover all information which may be linked to an individual and instances where personal data might be at risk. The identifiability criterion is therefore designed to cover all information likely to identify a natural person, even if traditional standards of identification have not been met.[11]

This interpretation of personal data is inherently "expansionist" and regarded as

*Lecturer, Department of Commercial and Industrial Law, Faculty of Law, University of Lagos Nigeria.
**Associate Professor, School of Law, University of Leeds (Corresponding author)
The authors wish to thank Prof Bert-Jaap Koops, Prof Jeanne Pia Mifsud Bonnici and Prof Philip Leith, who made helpful comments on an earlier draft of this paper.

[1] Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/2.

[2] 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 (Data Protection Directive) [1995] OJ L281/31

[3] Ibid, art 2(a)

[4] Although opinions of the WP29 are not binding, they are authoritative.

[5] Article 29 Working Party (WP29), 'Opinion 4/2007 on the Concept of Personal Data' (WP 136 20 June 2007), 6.

[6] Ibid, 15.

[7] Ibid, 14.

[8] WP 29, 'Privacy on the Internet – An Integrated EU Approach to On-line Data Protection' (WP 37 21 November 2000), 21.

[9] WP29, 'Opinion 13/2011 on Geolocation Services on Smart Mobile Devices' (WP 185 16 May 2011).

[10] WP29, Opinion 4/2007 (n 6) [15].

[11] Ibid [4-5].

fundamental to the protection of individuals.[12] However, it has given rise to a number of difficult conceptual and legal questions. One such question is the precise scope of the concept of data protection relative to the older concept of privacy and how to sustain the concept of personal data in the face of evolving technologies. This article will demonstrate that the definition of personal data is problematic for at least two reasons. First, the definition and its subsequent interpretations have blurred the fine lines between the concepts of privacy and data protection that had been drawn at the inception of the data protection regime. This blurring, which is primarily due to historical reasons in the EU, is also reinforced by the jurisprudence of the Court of Justice and the European Court of Human Rights. Hence not only is the definition of personal data and the propensity to expand its peculiarly European approaches, but the seeming global acceptability of this approach is questionable. Second, the article will argue that in any case, new developments in technology, particularly big data analytics (BDA),[13] Internet of things (IoT) and Artificial Intelligence (AI) make it difficult, if not impossible to maintain an expanding definition of personal data.[14] The article contends that concerning these technologies, the major problem is that the proliferation, combination and aggregation made possible by new technologies would render virtually any data *personal*. This, in turn, will make identification or identifiability routine and inevitable, potentially rendering the concept of personal data worthless if not nonsensical. Against this background, the central aim of this article is to challenge the status of EU law as the gold standard of data protection by demonstrating the inherent weaknesses in its central concept, personal data. The article also aims to force a reformulation of the concept that is adaptable to evolving technologies and applicable regardless of history or cultural relativeness of privacy.

The article is structured as follows; section one offers conceptual clarifications by examining the jurisprudence of privacy and data protection. It establishes the links between the identifiability criterion and the subjective notion of privacy in the EU and concludes that personal data defined in GDPR is neither a universal concept nor a reflection of privacy norms in other cultures and societies. For example, while the concept of privacy in Europe is linked to and forms part of personal dignity and personal image (Whitman refers to this as “dignitary privacy” or the linking of privacy and personhood),[15] in Africa,[16]collectivism, as opposed to the Western culture of individualism, is the prevalent culture of privacy. Accordingly, because Africans live in associations in which the individual is always part of the whole in relation to which his

[12] C Kuner, ‘Regulation of Transborder Data Flows under Data Protection and Privacy Law’ (2011) OECD Digital Economy Paper No. 187, 13.

[13] BDA entails the processing of the data using machine learning (ML) or algorithms that train the system on models of the world on which predictions can be made. The real value of BDA therefore lay in its capacity to make sense of data by drawing correlations or making predictions (predictive analytics). See M Neyer and D Laney, ‘The Importance of Big Data: A Definiton of Big Data’ (Gartner 2012) https://www.gartner.com/en/documents/2057415/the-importance-of-big-data-a-definition> accessed 09/02/2020 see also European Commission, ‘The EU Data Protection Reform and Big Data Factsheet’ (March 2016).

[14] See N Purtova, ‘The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10(1) Law Innovation and Technology 40.

[15] J Q Whitman,‘The Two Western Cultures of Privacy: Dignity Versus Liberty’ (2004) 113 Yale L.J. 1151, 1154-60.

[16] It is also applicable to Asian countries. Basu argues that privacy is more than just a simplistic legal concept beyond the normative questions addressed by western society, hence culture should simultaneously assert an exception and create opposition to a certain type of privacy rights, laws that are not in accord with the values of a particular society will be difficult to enforce. See S Basu, ‘Privacy Protection: A Tale of Two Cultures’ (2012) 6(1) Masaryk University Journal of Law and Technology,5, 1-34

or her existence is defined. An individual is never considered an entity unto oneself and is denied a space for claiming his/her right to privacy; there is an implicit de-emphasising of the notion of individualism in association with privacy in the African context.[17] However, many African countries are adopting EU law and its definition of personal data[18]. Therefore, we argue in this article that although the EU's individualistic approach to privacy has provided the underpinning for data protection legislation across the world[19] this account of privacy fails because it prioritises a single interest at the expense of others. As the article will demonstrate, this proposition is correct despite recent development that makes privacy and data protection separate and distinct fundamental rights under European law. Section two of the article considers the difficulties posed by new technologies for the concept of personal data. This section, using mostly examples of new technologies analyses how the pervasiveness of technologies with capacity for identification can lead to the proliferation of personal data and consequently, a loss of the value ascribed to such data. Section three examines different theories advocating alternative approaches to the definition of personal data and highlights and provides justifications for adopting a risk-based approach to defining personal data. The article finally argues in particular that while subjective harms (such as loss of dignity) are properly the subject matter of privacy laws, objective harms (such as fear of identity theft and fraud) should be the focus of data protection laws. In order to narrow the scope of personal data; however, an "objective risk of contextual harm"[20] which assess the risk of harm in the context of respective processing must be adopted. The section concludes with examples of how new data protection regimes may formulate alternative definitions of personal data.

## 2. How EU law conflates Data Protection and Privacy

The increasing number of data protection legislation in the world is either a testament to the importance of data protection globally[21] or a desire by many countries to qualify for trade with the EU by meeting its adequacy requirement.[22] This section will demonstrate that because the framing of personal data in the EU retains a connection to the notion of "dignitary privacy" and is influenced by peculiarly European history and experience of privacy as well as the socio-political and legal order in the EU, new and emerging data protection regimes ought to critically evaluate this definition when formulating their laws.[23]

---

[17] AB Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law 163, 168.

[18] Apart from All 28 countries of the EU including the UK when it leaves the EU (see Data Protection Act 2018 (UK) s 5), many other countries including Angola,, Argentina, Bahrain, Bermuda, Bosnia and Herzegovina, Brazil, Canada, cape Verde, Dominican republic, UAE, India, Nigeria, Zimbabwe and Zambia have all adopted definitions of personal data similar to the GDPR. for comprehensive list of countries that have adopted GDPR style laws and the definitions of personal data in their respective laws, see DLA Piper, Data Protection Laws of the World available https://www.dlapiperdataprotection.com/index.html?t=definitions&c=ZA&c2= accessed 09/02/2020

[19] K Sheehan, 'Towards a typology of internet users and online privacy concerns' (2002) 18(1) IS 21

[20] This is different from Nissembaum's theory which sets contextual integrity as the benchmark for understanding privacy expectations. See H Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Wash. L Rev, 101.

[21] About 120 countries now have comprehensive data protection laws following the EU omnibus approach. See G Greenleaf, 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey' (2017) 145 Privacy Laws & Business International Report, 10.

[22] See Commission (EC), 'Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World' COM (2017) 7 Final, 10 January 2017.

[23] Apart from All 28 countries of the EU including the UK when it leaves the EU (see Data Protection Act 2018 (UK) s 5), many other countries including Angola, Argentina, Bahrain, Bermuda, Bosnia and Herzegovina, Brazil,

The legal frameworks for privacy and data protection are encapsulated in a number of laws which are intricately related. The European Convention of Human Rights (ECHR) provides that everyone has the right to respect for his or her private and family life, home and correspondence and interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, or pursuit of meaningful and legitimate public interests and is necessary for a democratic society.[24] This provision is reiterated in Article 7 of the Charter for Fundamental Rights (CFR) of the EU, which further provides for a distinct right to the protection of personal data in Article 8. Conversely, one of the fundamental objectives of the GDPR and the EU Directive, arguably the most influential data protection law, is to protect the fundamental rights and freedoms of natural persons, and in particular their *right to privacy* concerning the processing of personal data. It is also notable that *Convention 108 for the Protection of the Individual with regard to the Processing of Personal Data*[25] (CoE Convention 108) contains a similar provision.[26] As stated in its preamble, the purpose of "Convention 108" is to secure in the territory of each "Party" for every individual, whatever his nationality or residence, respect *for his rights and fundamental freedoms,* and in particular *his right to privacy*, with regard *to automatic processing of personal data* relating to him. It is important to note that the seeming casual reference to privacy in some of the instruments cited above belies the historical connections and the complex and dynamic relationship between privacy and data protection. Although they have not always been helpful, attempts at conceptual clarifications between the two concepts is a useful starting point.

The right to privacy also dubbed the right to respect for private life in Europe,[27] consists of a general prohibition on interference, subject to some public interest criteria that can justify such interference in some instances. In Warren and Brandeis seminal article, '*the right to privacy*'[28], freedom from unwanted attention based on the principle of inviolate personality is at the core of privacy rights. 'The right to be let alone' thus ensured protection against unwanted disclosure of private facts, thoughts and emotions. Conversely, because the right to privacy *may be* lost when a person communicates information about himself to the public, real privacy is a peace of mind afforded by lack of publication[29]. As Prosser has argued, intrusion upon the plaintiff's seclusion or solitude, or into his private affairs is one of the four distinct torts comprising the right to be let alone.[30] Inherent in this exposition is the inference that a

Canada, cape Verde, Dominican Republic, UAE, India, Nigeria, Zimbabwe and Zambia have all adopted definitions of personal data similar to the GDPR. For a comprehensive list of countries that have adopted GDPR style laws and the definitions of personal data in the respective laws, see DLA Piper, 'Data Protection Laws of the World' <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=ZA&c2> accessed 09/02/2020.

[24] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (ECHR) art 8.

[25] The Convention was passed by the Council of Europe and opened for signature on 28 January 1981 and is still today the only binding international treaty in this field. It had considerable influence on the development of the EU data protection law.

[26] See CoE Convention 108 art 1.

[27] For some understanding of the rationale underlying the phrase, see European Commission of Human Rights, 'Preparatory Work on Article 8 of the European Convention on Human Rights' DH (56) 12, 9 August 1956 https://www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaux-ART8-DH(56)12-EN1674980.pdf accessed 09/02/2020.

[28] S D. Warren and L D. Brandeis, 'The Right to Privacy' (1890) 4(5) Harv L Rev, 193.

[29] W L Prosser, 'Privacy' (1960) 48(3) Cal L Rev, 383.

[30] Ibid, 389

right to be let alone entails a right not to be known or discovered or recognised, and the right not to disclose information about oneself or even the right to seclusion.[31] The ECHR has thus held that article 8 proscribes the communication of "personal information which individuals can legitimately expect should not be published without their consent" because it would damage their "honour" or "psychological or moral integrity" or "prejudice" their "personal enjoyment of the right to respect for private life."[32] In Post's recent assessment of Article 7 of the Charter of Fundamental Rights of the European Union (which corresponds to article 8 ECHR), he notes that the article protects the dignity of persons by regulating inappropriate communications that threaten to degrade, humiliate, or mortify them. Hence the notion of "dignitary privacy" which he argues follows a normative logic designed to prevent harm to personality caused by the violation of civility rules are the same privacy values as those safeguarded by the American tort of public disclosure of private facts.[33]

In contrast to (dignitary) privacy, the protection of personal data is a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed[34]. The right to informational privacy, often cast as data protection, follows Westin's alternative account of privacy in relation to significant changes in societies brought about by new technologies.[35] As Westin defines it, privacy is the claim of individuals, groups and institutions to determine for themselves, when, whether, how, and to what extent information about them is communicated to others.[36] Corresponding to this approach, European data protection law casts privacy as the right of individuals to control the collection and subsequent use of their information in an increasingly computerised society. In particular, data protection is described as a specific aspect of privacy that gives rights to individuals in how data identifying them or pertaining to them are processed and subjects such processing to a defined set of safeguards'.[37]Also, the notion of personal data is regarded as particularly helpful in discussing the relationship of privacy matters with technology because it leads to a relatively clear picture of what is the object of protection[38]. Perhaps to further underline the distinction between the two concepts, the Charter of Fundamental Rights (CFR) created a separate right to data protection in article 8 although the authorities had already proclaimed that protection of personal data must be seen as fundamental to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention.[39]

---

[31] Ibid, 389-407

[32] See *Axel Springer AG v Germany* (App No. 39954/08) ECHR [GC] 7 February 2012, [83]; see also *A v Norway* (App No. 280/06) ECHR 9 April 2009, [63].

[33] R Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere' (2018) 67 Duke L.J. 981, 982.

[34] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, and European Agency for Fundamental Rights, *Handbook on European Data Protection Law* (Publications of the European Union 2018 edn.), 19.

[35] AF Westin, *Privacy and Freedom* (Ătheneum, New York 1967) 7

[36] Ibid.

[37] C Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law' (2011) OECD Digital Economy Paper No.187, 13.

[38] J Van Den Hoven, 'Information Technology, Privacy, and the Protection of Personal Data' in M. J. Van den Joven and J. Weckert (eds.), *Information Technology and Moral Philosophy* (CUP, 2008).

[39] See European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Right: Right to Respect for Private and Family Life, Home and Correspondence' (Updated 31 August 2019) <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>;
see also *Marper v UK* (App nos. 30562/04 and 30566/04) ECHR 4 December 2008 [103].

As noted earlier, the attempts at conceptual distinction have been mostly unsuccessful. This is particularly so because of the dominant role of dignitary privacy in EU discourse and jurisprudence. Historically, the European notion of dignity has been a reaction against fascism, Nazism and discriminatory system in monarchical societies where only persons of high social status could expect their honour to be protected.[40] In Nazi Germany and other totalitarian regimes, for instance, personal data was used to identify members of disfavoured groups and in order to persecute them.[41] Thus, even when there is a lack of systematic link between the application of data protection rules and the right to privacy, the right to information self-determination pronounced in the 1983 landmark census ruling by Germany's highest court has been held to derive from the rights to human dignity, personal freedoms and free development of personality enshrined in the German Constitution or basic law.[42] The Court's definition of informational self-determination as the authority of the individual to decide fundamentally for herself, when and within what limits personal data may be disclosed is grounded in the view that processing of personal data interferes with dignity and personality rights already existing under German law.[43] It is instructive that the German state of Hesse passed the first modern data privacy law in 1970 and the Federal Data Protection Act followed it in 1977 and in 1983 the landmark decision declared that citizens have a right to informational self-determination. This historical backdrop provides an important context for the claim that the definition and interpretation of personal data under EU law probably derive from the older conception of dignitary privacy as either 'a right to be let alone' or a right to protection of private life. As already mentioned above, the GDPR and its predecessor, the Data Protection Directive, underline the protection of privacy as a fundamental motivation for data protection. The laws (and even the Convention 108, which predates them) defines personal data as information that relates to an identified or identifiable natural person. Article 29 Working Party (WP29) made it clear in its opinion on the interpretation and scope of the concept that identifiability is central to the designation of data as personal. It is therefore arguable that just as a person's right to be let alone is violated by knowledge of the person's personal (or even non-personal information), which he has not given, so is his right violated when the processing of data on computerised systems allow him to be known or identified. In other words, the only way that identifiability becomes relevant in the context of data protection is if it is seen through the lens of a right to be let alone. Presumably, if a person has a right to be let alone, he also has a right not to be identified as a critical component of the protection of his dignity and personhood.

As the WP29 further clarified, a person is "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group[44]. Such distinction is

[40] Whitman, (n 16) 1151, 1164-71.

[41] See J Santoli, 'Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive' (2008) 40 Geo. WASH. INT'L REV. 553, 556.

[42] See e.g. O Lynskey, 'Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order' (2014) 63(3) International and Comparative Law Quarterly, 569, 572; see also A Freude and T Freude, 'Echoes of History: Understanding German Data Protection' https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/ accessed 09/02/2020.

[43] 65 BVerfGE 42 (1984) cited in EJ Enerle, 'Observation of the Development of Human Dignity and Personality in German Constitutional Law: An Overview' (2012) 33(3) Liverpool Law Review, 201, 225; see also S Simitis, Privacy-An Endless Debate (2010) 98 Cal. L. Rev. 1989, 1990.

[44] WP29 Opinion 4/2007, (n 6) 12.

typically achieved through "identifiers", that is, particular pieces of information which hold a particularly privileged and close relationship with the particular individual[45]. Significant examples given include outward signs of appearance, such as height, hair colour, clothing, and even a name[46]. In fact, as the WP29 noted, concerning "directly" identified or identifiable persons, the name of the person is indeed the most common identifier, and, in practice, the notion of "identified person" implies most often a reference to the person's name.[47] Therefore it would seem that when it comes to "identified", the data can be self-executing, everyday identifiers. On the other hand, since attributes, such as names and physical features that distinguish an individual are hardly sacrosanct, it can be argued that identification is not at stake as the individual has been identified pre-data processing using the same attributes. In other words, an intuitive inclination to protect identity is perhaps the only explanation for bringing "identified" within the rubric of data protection laws. This intuition is fuelled by a presumption that we have a right not to be identified. However, as Thomson argued many years ago; we neither have a right not to be looked at nor right against others that they will not know information about us simply because we have a right to privacy.[48] As she asserts, '*…none of us has a right over any fact to the effect that others shall not know the fact. [And while it is possible to] violate a man's right to privacy by looking at him or listening to him; there is no such thing as violating a man's right to privacy by simply knowing something about him. Where our rights in this area do lie is, … we have a right that certain steps shall not be taken to find out facts, and we have a right that certain uses shall not be made of facts*'[49]. If it is correct that we do not have a right not to be looked at or that others should not know facts about us, ultimately, it is the use to which the data is put that matters and not the fact of identification which must be considered a given. This is perhaps why the WP29 itself further opined that "identifiable" rather than identified is in practice the threshold condition determining whether the information is within the scope of the third element, that is identified or identifiable natural person.[50] Following the same track, European Courts have also consistently conflated data protection and privacy and treated the former as an extension of the latter. Apart from a handful of cases, for example,[51] the decisions of the Court of Justice are permeated by a "privacy thinking"[52] which manifested itself in how the Court undertakes the very construction of the right to personal data protection as a sui generis or unique right.[53]

In *Breyer*,[54] (which is a post CFR case) it is clear that the primary question before the Court did not call for a consideration of whether IP addresses interfere with private life as such, but simply whether the data itself constitute personal data. Thus, in finding that IP addresses do constitute personal data, the Court demonstrated that

[45] Ibid.

[46] Ibid, 12-13; see also Case C-101/01 *Bodil Linqvist* (2003) I-12971, [24], [27].

[47] WP29 Opinion 4/2007 (n 6) 13.

[48] JJ Thomson, 'The Right to Privacy' (1975) 4(4) Philosophy & Public Affairs, 295, 312.

[49] Ibid, 307.

[50] WP 29 Opinion 4/2007 (n 6) 12.

[51] See e.g. Case C-293/12 *Digital Rights Ireland* Case (ECR [GC] 8 April 2014) [26]-[36] where the Court made a seeming distinction between privacy and data protection.

[52] See G G Fuster and R Gellert, 'The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right' (2012) 26(1) International Review of Law, Computer and Technology 72, 73.

[53] Ibid, 79-80.

[54] Case C-582/14 *Breyer v Bundesrepublik Deutschland* (ECJ 19 October 2016).

consideration of whether data is personal could be done in isolation of its private life implications. Nevertheless, the Court could not resist a reference to private life interests which in its opinion are implicated by dynamic IP addresses. As the Court noted, merely by providing information on the date and time of accessing a web page from a computer (or other devices), dynamic IP addresses show some patterns of Internet users' behaviour and therefore involve a *potential interference with the right to respect for private life*[55]. By this opinion, the court appears to suggest that there must be an interference with the right to privacy every time data is processed.[56]

Similarly, in *Volker*,[57] the court held that there are no practical differences between the right to privacy and the right to protection of personal data as the Articles 7 and 8 rights both concern 'any information relating to an identified or identifiable individual'[58]. Following the reasoning in *Rundfunk*, the Court then held that the two rights are subject to similar restrictions and the same proportionality test. In other words, it must be considered that the limitations which may lawfully be imposed on the right to the protection of personal data (under Articles 7 and 8 of the Charter) correspond to those tolerated in relation to Article 8 of the Convention[59]. Notably, in *Rundfunk,*[60] the Court made it clear that the provision of the (Data Protection) Directive requiring fundamental respect for private life concerning the processing of personal data means that the Directive must be interpreted in the light of privacy rights guaranteed by the European Convention of Human Rights (ECHR). Therefore, to apply Directive 95/46, and in particular Articles 6(1)(c), 7(c) and (e) and 13, it must be ascertained, first, whether legislation such as that at issue in the main proceedings (that is the Austrian national law requiring the collection and publication of data relating to professional income above a designated threshold) provides for an interference with private life, and if so, whether that interference is justified from the point of view of Article 8 of the Convention[61].

The older cases suggest that the Court's reasoning was the same before the Charter came into effect. In *Rijkeboer*,[62] the Court held that the purpose of the Data Protection Directive was to protect the privacy of individuals. This position is seemingly in conflict with Articles 1 paragraphs (1) and (2) of the Directive which defines the objective of the directive and provides that the Member States may neither restrict nor prohibit the free flow of personal data between the Member States for reasons connected with the protection of the fundamental rights and freedoms of natural persons, in particular, their private life, with respect to the processing of that data. In *Lindqvis*t, the Advocate-General had argued that the Data Protection Directive has dual objectives and the

---

[55] Ibid [55] (emphasis).

[56] Note that before the decision in *Breyer*, there was a general lack of consensus among member states on the status of IP address. This was perhaps because the different European countries were unable to find the precise privacy interests implicated by the processing of IP addresses see e.g. ICO, 'Personal Information Online Code of Practice',https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf accessed 17/03/2016; See also *EMI Records (Ireland) & Ors v Eircom Ltd* [2010] IEHC 108,16-25.

[57] Joined Cases C-92/09 and C-93/09 *Volker and Markus Schecke GBR and Hartmut Eifert v. Land Hessen* (2010) ECR I-11063.

[58] Ibid [52].

[59] Ibid [58]-[59], [64]-[89].

[60] Joined cases C-465/00), C-138/01, C-139/01 *Osterreichischer Rundfunk & ors* (ECJ 20 May 2003)

[61] Ibid [72].

[62] See Case C-553/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* (2009) ECR I-03889.

protection of the fundamental right to privacy is a secondary, and not a primary objective of the Directive[63]. This opinion is consistent with the notion that data protection is founded in society's need to address the threats of organisational abuses of personal data, and its effect is to shift responsibility for the protection of personal information "to the greatest extent possible" from individual data subject to third party handlers of data.[64] Nevertheless, the Court held that the mere mention of a person by name constitutes processing of personal data.[65]

Decisions of the ECtHR also provide insights into the reasoning of the court on the relationship between privacy and data protection and the scope of the respective concepts. For example, while the ECHR does not have a provision corresponding to Article 8 of the Charter,[66] the CoE asserts that several provisions of the ECHR, particularly Articles 8 and 10, are relevant to 'the protection of individuals with regard to automatic processing of personal data'[67]. Also, the ECtHR itself has noted that it defines article 8 broadly to cover even rights that are not explicitly set out in the article. The Court has thus extended Article 8 to cover the protection of personal data.[68] In *Marper v UK*,[69] the Court held that Article 8 is applicable because storage and retention of personal data (DNA and fingerprint samples) in the case constitute a disproportionate interference with the applicants' respect for private life which cannot be regarded as necessary in a democratic society.[70] In *Amann v Switzerland*,[71] the Court held that its broad interpretation of "private life" corresponds with that of the CoE Convention 108 whose purpose is to secure in the territory of each Party for every individual respect for his rights and in particular his right to privacy, with regard to automatic processing of personal data relating to him. Such personal data is defined as 'any information relating to an identified or identifiable individual'.[72]

In the more recent case of *Antovic and Mirkovic v Montenegro*[73], the ECtHR missed the opportunity to provide the much-needed answer to the recurring question of how and the extent to which data protection overlaps privacy. The question in the case was whether article 8 ECHR applies to video surveillance in a University auditorium where the applicants, two professors, teach their students. Although the Court found by a

---

[63] Case C-101/01 *Bodil Lindqvist* Opinion of Advocate General Tizzano ECR (2003) I-12971 [40].

[64] F H Cate and V Mayer-Schonberger, 'Tomorrow's Privacy Notice and consent in a World of Big Data' (2013) 3(2) International Data Privacy Law 67, 70.

[65] *Bodil Lindqvist* (n 47) [20]-[27].

[66] Article 8 CFR provides as follows; 'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.'

[67] Council of Europe, 'Explanatory Memorandum to Recommendation No. R (2002) 9 of the Committee of Ministers to Member States on the Protection of Personal Data Collected and Processed for Insurance Purposes' (18 September 2002), 2.

[68] See Guide to Article 8 of the ECHR (n 40) 7.

[69] (App nos. 30562/04 and 30566/04) ECHR 4 December 2008.

[70] Ibid [67], [125]-[126]; see also *Barbulescu v Romania* (App no 61496/08) ECHR [GC] 5 Sept 2017, [70]-[81]. where the court held that the term private life is a broad term not susceptible to exhaustive definition and includes applicants communication in the workplace.

[71] (App No. 27798/95) ECHR 16 February 2000.

[72] *Amann v Switzerland* (Application No. 27798/95) ECHR 16 February 2000 [65]; see also *Barbulescu v Romania* (n 71); *Rotaru v Romania (*App No. 28341/95) ECHR 4 May 2000 [43]– [44].

[73] Antović and Mirković v Montenegro [2017] ECHR 28 November 2017.

majority of 4 to 3 that video surveillance of an employee in the workplace, be it covert or not, must be considered as a considerable intrusion into the employee's private life which constitutes an interference with Article 8,[74] the dissenting judgement is much more significant for highlighting the blurring lines between data protection and the right to respect for private life. The minority concurred with the judgement in so far as it concludes that the interference in question was not in accordance with the law and therefore constituted a violation of Article 8.[75] However, the judges disagreed with the declaration that the application is admissible and the finding of a violation of Article 8 of the Convention. Contending that the case law forces a distinction between monitoring or surveillance as such and the *recording, processing and use of the data obtained*[76]*,* the Judges argue that in determining whether surveillance interferes with private life, the majority ought to take into account not only the fact of the surveillance itself but also the *recording, processing and use of the data obtained*[77]*.* The Judges were of the view that the majority reached its decision because it focused on the video surveillance as such without considering the further factors that determine whether there was, in fact, interference with private life and this interpretation in their views unduly broadened the scope of Article 8[78].

The central argument made by the dissenting judges is that while the use of the surveillance cameras did not interfere with the right to respect for private life, it raises issues of data protection including the extent to which the recording qualifies as processing of personal data and comply with the principles of data protection. This case, therefore, provides significant insights into the data protection/right to private life dichotomy. On the one hand, by holding that surveillance per se does not raise issues of interference with private life, the dissenting Judges suggest that processing of personal data can take place without the same implicating privacy or private life. Therefore, in terms of overlap, the processing of personal data does not immediately provoke privacy or the right to private life response. On the other hand, surveillance per se immediately has data protection implications because it may involve the processing of data relating to an identified or identifiable person, with the consequence that the principles of data processing automatically kick in.

It is important to mention that overall, the Court of Justice has itself admitted that the privacy jurisprudence of the EU differs from that of other countries. In striking down the safe harbour agreement in Schrems, the Court observed that while in the US, government surveillance including access to personal data is extensive and even permissible by law, under EU law, 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.' [79]

Following this point, it is arguable that if the understandings of privacy in the EU influenced the definition of personal data, then third countries adopting EU-style law and its definition of personal data do so without an assessment of the socio-cultural

[74] Ibid [44], [55], [68].
[75] Ibid [56]-[60] Joint Concurring Opinion of Judges Vucinic and Lemmes [1]-[6].
[76] Ibid Joint Dissenting Opinion of Judge Spano, Biaanku, Kjolbro [7]-[9].
[77] Ibid.
[78] Ibid [9]-[10].
[79] See Case C-362/14 *Maxmillan Schrems v Data Protection Commissioner* (ECR [GC] 6 October 2015) [94].

perceptions of privacy and how this may be relevant to a determination of the scope of personal data and the administration and enforcement of the law.[80] While Rodota cautions against equating the defence of (European) model of data protection to a defence of the Europeans' interests because other countries and different cultural environments also support the model,[81] however more recently Kuner attributed the global success of EU law to other factors. As he argued, the success of the law is due in part to the perceived economic benefits that can accrue to third countries that adopt the EU as a model law[82]. That is that they can import personal data under European adequacy decision (although there is no verifiable evidence that EU adequacy decisions lead to economic growth).[83] In part, the success can also be attributed to the convenience that a set of clearly-structured ready to use model law offers over drafting new legislation from scratch. In line with, Bradford we also argue, although, the EU's external regulatory agenda (referred to as the "Brussels effect") may not be the result of a conscious effort to engage in "regulatory imperialism", the unilateral regulatory globalisation achieved by the EU is partly a result of Europe's market power.[84]

A further point to note is that the EU itself now seems to recognise the conundrum created by its continued reference to privacy in specific incompatible contexts. Accordingly, the EU Charter of Fundamental Rights framed the right to protection of personal data as an autonomous fundamental right in its article 8. Although the Charter remains the first and only instrument in this respect, recent legislative instruments including the GDPR and the Convention 108+ appeared to have followed its example. The Convention now refers to a right to protection of personal data, and in article 1 now states that 'the purpose of this Convention is to protect every individual, whatever his or her nationality or residence, *with regard to the processing of their personal data*, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy. The GDPR also provides in Article 1 that 'this Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the *protection of personal data'.* While it remains unclear whether and how a new fundamental right to personal data and a change in nomenclature (from privacy to data protection) would herald a new jurisprudence of data protection, it is clear that the EU law now considers the interchangeable use of privacy for data protection an anomaly.

---

[80] For alternative accounts of privacy, see e.g. J Q Whitman (n 41); see also A Etzioni, 'The Limits of Privacy' in A I Cohen and C H Wellman (eds) *Contemporary Debates in Applied Ethics* (Blackwell Publishing 2005) 253; L A Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) Stockholm Institute for Scandinavian Law 166; S Basu, 'Privacy Protection: A Tale of Two Cultures' (2012) 6(1) Masaryk University Journal of Law and Technology 1-34

[81] See S Rodota, 'The European Constitutional Model for Data Protection' (March 2007). Paper presented at the public semnar of the European Parliament: PNR/SWIFT/Safe Harbour: Are transatlantic data protected? (Transatlanitc relations and data protection)
http://www.europarl.europa.eu/hearings/20070326/libe/rodota_en.pdf accessed 12/11/2019.

[82] C Kuner, 'The Internet and Global Reach of EU Law' (2017) LSE Law, Society and Economy Working Papers 4/2017, 18

[83] It has been argued for example that not only is the GDPR unsuited for the specific needs of developing countries, but also, as a global framework for data protection, the GDPR does not support digital trade. See A Mattoo and J P. Meltzer 'International Data Flows and Privacy: The Conflict and its Resolution' (2018) 21 Journal of International Economic Law 769, 772.

[84] A Bradford, 'The Brussels Effect' (2012) 107(1) Nw. U. L. Rev. 1, 2, 22-26.

In the next section, it is argued that apart from the influence of EU privacy jurisprudence on the definition of personal data, developments in technologies also make it difficult to sustain the current concept of personal data.

## 3. New Technologies and the Concept of Personal Data

The objective of the broad approach to interpreting personal data is to protect not only information considered personal already but also those that may become potentially personal. Its main advantage is flexibility, which implies that new forms of personal information created by new technologies could fall within its ambit. However, flexibility also means the definition of personal information is open-ended, unstable and ambulatory. The challenges created by "Big data analytics" (BDA), the IoT and AI applications provide good examples. BDA analyses all data to find a correlation, and can produce or generate 'new' and 'unusual' personal data.[85] For example users' 'likes' on Facebook has been shown to reveal information on sexual orientation, ethnicity, intelligence, religious and political views, personality traits, happiness, use of addictive substances, parental separation, age and gender.[86] The same research found that liking curly fries is indicative of high intelligence[87] while another research found that computer predictions based on a generic digital footprint (the Facebook Likes) are more accurate than those made by the participants Facebook friends using a personality questionnaire.[88] As the ICO also observed, because the data being used for analytics has been generated automatically by tracking online activity,[89] and big data need not rely on having a person's personal data directly but on a combination of techniques from social network analysis, interpreting online behaviours and predictive modelling can create detailed profiles that have a high level of accuracy.[90] According to the UNHRC, when aggregated, metadata can reveal personal information that is no less sensitive than the actual content of communications and these can give an insight into an individual's behaviour and social relationships, as well as private preferences and identity.[91]

There are two significant problems here. Firstly, BDA underpins the lack of correlation between the indicative data (such as Facebook 'likes') and predictive attributes (such as intelligence, happiness or substance abuse). This means in effect that any data, however ubiquitous or remote, can be linked to a person and with a high degree of precision. Surely, in this case, there is very little to be gained by protecting a species

[85] ICO, Big Data, 'Artificial Intelligence, Machine Learning and Data Protection' (2017) https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [19]-[20].

[86] M Kosinski, D Stillwell and T Graepel, 'Private Traits and Attributes are predictable from Digital Records of Human Behavior' 'https://www.pnas.org/content/pnas/early/2013/03/06/1218772110.full.pdf, accessed 09/02/2020.

[87] Ibid.

[88] Wu Youyou, M Kosinski and D Stillwell, 'Computer-based Personality Judgments are more Accurate than those made by Humans' (2015) 112(4) PNAS, 1036.

[89] ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection' (2017) [19] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf,accessed 09/02/2020.

[90] K Crawford and J Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) New York University School of Law Public Law & Legal Theory Research Paper Series, Working Paper No. 13 -36, 93.

[91] UNHRC 'The Right to Privacy in the Digital Age' (7 April 2017) UN Doc A/HRC/RES/34/7, 3; see however the decision of the Australian Federal court in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4, [6], where the court held that metadata is not personal data as it does not qualify as data about an individual in the definition of personal information under the Australian Privacy Act.

of data as personal. Secondly, since it would be difficult to determine with any level of precision that personal data can be generated in any particular processing context, then applicable principles of personal data will have to be applied *ex-post* (or after the fact of the processing). This would create difficult if not insurmountable compliance hurdles for organisations that must comply with the law. [92]

IoTs raise similar problems. IoTs rely on the principle of extensive processing of data through sensors that are designed to communicate unobtrusively and exchange data in a seamless way. They are closely linked to the notions of "pervasive" and "ubiquitous" and "ambient" computing.[93] While transmitting information about connected things, therefore, IoTs also invariably transmit information about their users. Sensors in smart cars provide vast amounts of data about the car as well as about the patterns in people's driving behaviour (which can help to inform decisions about their insurance premiums).[94] Personal and household devices such as smart meters, smart refrigerators and wearables, can transmit information about their owners' preferences, lifestyles, gender, and health status. In the context of IoT, therefore, it is often the case that an individual can be identified based on data that originates from "things". Indeed, data -such as those generated by centralised control of lighting, heating, ventilation and air-conditioning- can allow discerning of the life pattern of a specific individual or family.[95] Based on the exponential growth of IoT (projected to hit 50 billion connected devices by 2020),[96] most IoT generated data qualify as personal data (particularly because BDA can generate identifying data without any correlation between indicative and predictive data).

In the case of AI applications,[97] "deep learning", a set of autonomous and self-learning algorithms, at the core of the applications, optimises predictive reasoning that allows AI systems to learn and adapt.[98] A particular challenge of algorithmic processing of personal data is, therefore, the generation of new data which may occur when a data subject shares a few discrete pieces of data which may be merged to generate second and even third generations of data about the individual. Moreover, innocuous pieces of data, when assessed in comparison with a much larger data set can "breed" and generate "baby data", the nature of which can be entirely unpredictable for the data subject and which raises major issues for the concepts of consent, transparency and personal autonomy.[99] In other words, since AI is ultimately about giving computers behaviours which would be thought intelligent in human beings, and systems'

[92] ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection' (n 90) [15], [19], [20].

[93] WP29, 'Opinion 8/2014 on the Recent Development on the Internet of Things' (16th Sept. 2014), 4.

[94] ICO, Big Data and Data Protection, https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220, [38].

[95] WP29, Opinion 8/2014 (n 94) [10]-[11].

[96] See e.g. Gatner, 'Gartner Says 8.4Billion Connected Things will be in use in 2017, Up 31% from 2016' https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 accessed 09/02/2020.

[97] The OECD defines AI system as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.' See OECD, 'Recommendations of the Council on Artificial Intelligence' (adopted 22/05/2019) OECD/Legal/0449.

[98] See P Boucher, 'How Artificial Intelligence Works' (March 2019) European Parliamentary Research Service PE 634.420http://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-how-artificial-intelligence-works.pdf accessed 09/02/2020.

[99] See Council of Europe, 'Algorithms and Human Rights' (Council of Europe Study DGI 2017 12) [13] https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 accessed 09/02/2020.

designers need not foresee or provide solutions for all possible situations because fully autonomous, or unsupervised AI can make decisions that are not derived from the original data or specified in advance, it would become virtually impossible to predict whether personal data will be created or whether the results from analytics would be meaningful or correct.[100] One example of the complex problem here is the seeming right to an explanation of algorithmic decision-making in the GDPR.[101] It has been argued, and quite rightly that the right (if indeed it exists)[102] poses a real danger of creating a "meaningless transparency" paradigm to match the already well known "meaningless consent" trope.[103] This is not only because automated, algorithmic decision-making is usually difficult to predict for a human being and its logic difficult to explain after the fact,[104] but also because the right to explanation may be significantly overrated or even irrelevant in many cases. Edwards and Veale further point out that case law and incidents relating to algorithmic decision making have shown that data subjects do not want an explanation, rather what they want is for the decision or action not to have occurred at all.[105]

Another example is the provision of anonymisation. Although article 26 GDPR recommends anonymisation and pseudonymisation to render data non-personal and provides that the Regulation "…shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable", it is clear that the circumstances in which the data subject will not be identified are becoming increasingly narrow and constrained. If we concede for example, that AI systems can be autonomous or that they have the cognitive capacity, we must ask whether data can be truly anonymised, pseudonymised or forgotten? Would a system unlearn (or forget) what it has learnt from the data or if the system 'forgets' (or is made to forget) can it still pull information from different sources to rebuild a profile that has been forgotten to de-anonymise an anonymised identity?[106] While it seems impossible to eliminate the risk, the Article 29 Data Protection Working Party (regarding anonymisation techniques), partly conceptualises anonymisation as requiring a zero (or near-zero) probability of reidentification which suggests that re-identification must be "irreversible."[107]

---

[100] See European Group on Ethics in Science and New Technologies, 'Statement on Artificial Intelligence, Robotics and Autonomous Systems' (March 9 2018) [7] http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf accessed 09/02/2020.

[101] See GDPR arts 22, 13, 14,15, see in particular recital 71.

[102] See e.g. S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law, 76, 77, 79-84 arguing that the GDPR does not implement a right to explanation for algorithmic decision making in its current form. See however, M E Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkely Technology Law Journal 189, 193, arguing that the GDPR infact creates an algorithmic accountability regime that is broader and stronger than what existed under the EU's Data Protection Directive (DPD). See also Algorithmic Accountability Act (US) 2019 and the European Parliament, 'A governance Framework for Algorithmic Accountability and Transparency' (April 2019) http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf, accessed 09/02/2020.

[103] L Edwards and M Veale, **'**Slave to The Algorithm? Why A 'Right to An Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16(1) Duke Law and Technology Review 18, 23, 33.

[104] See Council of Europe, 'Algorithms and Human Rights' (n 100) 6.

[105] Edwards and Veale (n 104) 42-43.

[106] See e.g. ICO, 'Big Data and Data Protection', https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220 [42].

[107] I Rubenstein, 'Brussels Privacy Symposium on Identifiability: Policy and Practical Solutions for Anonymisation and Pseudonymisation, Framing the Discussion' https://fpf.org/wp-content/uploads/2016/11/Rubinstein_framing-paper.pdf 9-10, accessed 09/02/2020.

Unsurprising, while one scathing assessment of the GDPR is that it risks becoming a "law of everything" which in theory aims to deliver the highest legal protection under all circumstances but impossible to comply with in practice because its scope is unreasonable.[108] This however usefully draws attention to another criticism of the law is that it sets normative preferences in tension with information-intensive industry practices, and in it lies great tension with big data and machine learning business models, at least in their current forms.[109]

It is arguable, following the above analysis that the proliferation of personal data could undermine data protection regimes by calling into question the value that personal data protects.[110] Dror has argued that it is impossible to assign meaning to any part of the law and apply the same to concrete cases without regarding the purpose (or purposes) which that part of the law is designed to serve[111]. The purpose also constitutes the value(s) reflected in the law, which in some cases, is easy to discern and, in some others, difficult. The prohibition of murder, for instance, is directed at safeguarding human life and the main value expressed in the law is the sanctity of human life. Similarly, the prohibition of theft has as one of its purposes the protection of private property,[112] and we can argue that the protection of privacy and personal data are linked to the core value of human dignity and autonomy. According to European Data Protection Supervisor (EDPS) for instance, privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing. Thus in Germany, the right to 'informational self-determination' was based on the rights to personal dignity and to free development of the personality laid down in Articles 1 and 2 of the German Constitution.[113]However, the correct explication of human dignity (at least in the context of rights such as privacy) is that it entails a choice.[114] This would imply that disclosing one's information or choosing who knows the information is as much an exercise of one's dignity as withholding or excluding certain people from knowing that information. As HLA Hart rightly noted, the right holder's ability to choose freely from a variety of acceptable options in life and to what she will do freely is common to any species of the right to liberty'.[115]

The above also suggests that the value attached to personal data would depend on respective views of individuals, groups or cultures. We could, therefore, create a value gap if we cannot link certain information to our sentiments or beliefs about human (in)dignity. We may argue for example that not only is it freedom and equally dignifying

[108] Purtova (n 15) 40 -41.

[109] C J Hoofnagle, Bart van der Sloot and F Z Borgesius, 'The European General Data Protection Regulation: What it is and What it Means' (2019) Information and Communication Technology Law, 65, 72.

[110] Purtova, (n 15) 40.

[111] Y Dror, 'Value and the Law' (1957) Antioch Review 440, 441-442.

[112] Ibid.

[113] European Data Protection Supervisor (EDPS), 'Towards a New Digital Ethics: Data, Dignity and Ethics Opinion 4/2015 (11 September 2011) 12.

[114] See e.g. L Floridi 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philos. Technol. 307.

[115] H. L. A. Hart, *Bentham on Legal Rights* in A. W. B. Simpson (ed),*Oxford Essays on Jurisprudence*, (Oxford: Clarendon Press, 2nd Series 1973),171-201 cited in A Corlett, 'The Nature and Value of the Moral Right to Privacy'(2002) 16 (4) Public Affairs Quarterly, 329, 331.

if algorithms make our choices,[116] but also that ubiquitous information such as the temperature in our home or the functioning of home-based appliances have no link to our dignity in particular when effective functioning of the devices are dependent on the collection of such data.[117]

The criticisms that have trailed the declaration of data protection as a fundamental right in Europe is particularly instructive in this regard. For example, Lynskey points out that there is a lack of clarity regarding the objectives of the right to data protection and this calls into question the global application of its data protection standards which in turn detracts from the legitimacy of the EU data protection regime.[118] Thus the right (to data protection) is necessarily procedural in so far as it 'does not directly represent any value or interest per se and only prescribes the procedures and methods for pursuing respect of values embodied in other rights'[119]. The right is such that there is no threshold for the application of data protection rules, as is common with human rights instruments and as both essential and non-essential interests are provided protection, data protection is akin to market regulation than to the human right.[120] By the same logic, personal data has been criticised for having a scope that does not fit the classical scope of human rights.[121] While on the one hand, there are certain cases such as those revealing a person's sexual or political orientation, medical conditions or race, that could qualify as fundamental rights and are essential in a democratic society, there are others such as names, addresses and shopping habits on the other hand, which seem less apparent candidates for fundamental rights protection because they protect more ordinary interests and intuitively do not qualify as (part of) a fundamental (human) right.[122] In other words, since human rights are intended to protect the essential values of human life and liberal democracies, an infinite concept of personal data means the law protects very insignificant interests on the same level as fundamental rights. Protecting these small interests of consumers under the realm of the fundamental rights, however, means that limitations and infringements on such interests become increasingly common and having a fundamental right would have no or very little added value over having a normal right. The UK ICO gives an example which illustrates this point as follows; 'a nursery produced Father's Day cards for the children to take home. Within the card was a photo of the child. There were two children with the same name at the nursery, which accidentally put child A's photo in

[116] G Buttarelli, 'Choose Humanity: Putting Dignity back into Digital' (Opening Speech of Debating Ethics Public Session of the 40th Edition of the International Conference of Data Protection Commissioners 24 October 2018),12 https://www.privacyconference2018.org/system/files/2018-10/Choose%20Humanity%20speech_0.pdf. Accessed 09/02/2020.

[117] E.g. Google's defence to revelations that its contractors listen to recordings on its AI system, Google Assistant, was that it helps the system to better understand patterns and accents and while the feature can be turned off, doing so means Assistant losses much of its personalised touch. see Google 'Workers can Listen to what People say to its AI Home Devices' the Guardian, Thursday 11 July 2019 https://www.theguardian.com/technology/2019/jul/11/google-home-assistant-listen-recordings-users-privacy accessed 09/02/2020.

[118] Lynskey, (n 43), 573.

[119] Norberto Nuno Gomes de Andrade, 'Oblivion: The Right to Be Different ... from Oneself Reproposing the Right to be Forgotten' (2012) Monograph VII International Conference on Internet, Law & Politics Net Neutrality and other challenges for the future of the Internet, 122, 125 https://pdfs.semanticscholar.org/f3ad/3b8c32883cced368fd244f4b8ed0cc232931.pdf accessed 09/02/2020

[120] B Van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in R. Leenes, R. van Brakel, S. Gutwirth, and P. De Hert (eds.), *Data protection and Privacy: (In)visibilities and infrastructure* (2017) 36, Law, Governance and Technology Series, 18-19.

[121] Ibid, 20.

[122] Ibid, 15.

child B's card and vice versa'. Although the ICO concluded that the breach was not reportable and no further action was required because it is unlikely that individuals' rights and freedoms would be impacted by the wrong photo being sent out, the example shows how extending the definition of personal data can diminish the value of fundamental rights. [123] This approach could mean that fundamental right could become a hollow concept, and with time, not only privacy and data protection but all fundamental rights will lose their special status.[124] As the Centre for Information Policy and Leadership at Hunton & Williams LLP noted, it is no longer enough—or sufficiently meaningful—to say solely that privacy is a human right and that the laws exist to safeguard "fundamental rights and freedoms", nor that they are confined solely to existing privacy principles or fair information practices. New times call for new clarity and new pragmatism.[125] Perhaps this is why the EDPS has noted more recently that the concept of 'personal data protection' will disappear in the near future, as will the concept of 'personal data'. We will all be easier to predict and identify even without data about our individual identities, and it will be easier to reuse the information and group it together with other information and interpret it accordingly'.[126] The EDPS, therefore, advocated that law alone cannot safeguard human rights in the digital age and regulators should start looking at developing a coherent (global) ethical framework in the area of privacy protection.[127]

## 4. A new definition of personal data – The theory of Harm

It has been argued above that the definition of personal data in the GDPR is influenced by experiences and socio-cultural conceptions of privacy in the EU. Apart from cultural relativity, however, the concept is also infinite if not meaningless in a technological context. In the light of the preceding discussion, this section critically analyses alternative concepts of personal data and argues in particular that a definition based on an objective risk of (contextual) harm corresponds to the niche area of data protection, takes account of different notions of privacy and delimits the scope of personal data in the face of evolving technologies.

### A. A Risk of Harm approach

Proponents for the adoption of risk of harm as a basis for defining personal data take a different approach. According to Hon et al.,[128] a two-stage technologically-neutral, accountability-based approach should be adopted to minimise identification risks.[129] The first stage is based on a risk of identification. At this stage, it is proposed that

[123] ICO, 'GDPR One Year on' https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf accessed 09/02/2020.

[124] Van der Sloot, (n 121) 19.

[125] Centre for information Policy and Leadership, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (19 June 2014), 2 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf accessed 09/02/2020.

[126] R Zangrandi 'I'm sorry my Friend, but you're Implicit in the Algorithm…' Privacy and Internal Access to Big Data Stream: An Interview with Giovanni Buttarelli, European Data Protection Supervisor' http://www.digidig.it/2016/11/20/now-in-english-a-conversation-with-the-european-data-protection-supervisor/ accessed 09/02/2020.

[127] Buttarelli, (n 117) 14.

[128] W K Hon, C Millard and I Walden, 'The Problem of 'Personal Data' in Cloud Computing: What Information is regulated? The Cloud of the Unknowing' (2011) 1(4) International Data Privacy Law 211, 214-222, 227-228.

[129] Ibid.

appropriate technical and organisational measures should be taken to minimise the risk of identification. It is, therefore, only if the resulting risk remains sufficiently high that data should be considered personal. The second stage proceeds to assess the risk of harm identified in the first stage and its likely severity. If sufficiently severe, appropriate measures must be taken, regarding the personal data, with obligations being proportionate to risks.[130]

The problem with the expansionist approach is that it creates a continuum of risk which equates identified information with identifiable information[131]. Hence to break the continuum, Schwartz and Solove suggested a differential application of standards of fair information practices (FIPs) (or data protection principles) based on a risk of harm which is dependent on whether the information is identified or identifiable[132]. In this respect, they identified three categories of personal information as identified, identifiable and non-identifiable information and proposed that for identified personal data, all FIPs should apply, because this data already relates to a known individual and carries a higher risk of harm. For identifiable information, only the core principles of FIPs, particularly data quality, data security and transparency should apply.[133] This is because identifiable information is yet to relate to a specific individual and may never do so. No FIPs should apply to non-identifiable information because they are not relatable to any person taking into account all means likely to be used for identification.[134]

The above proposals are persuasive but are generally complicated. They are persuasive because, in contrast to the disconnected notion of identifiability promoted by the EU expansionist approach, they take cognisance of a real risk of identification as well as the notion and possibility of harm resulting from the identification process. The complexity, however, derives from the multi-stage or multi-level assessment and application proposed by the authors. For example, Schwartz and Solove proposed model suggests that information which was at first unidentifiable may later become identifiable. Once identifiable, the information triggers the application of all FIPs.[135] This makes it difficult to see how the scope of the concept can be narrowed even by reconceptualising personal information. Arguably, it merely produces a circular process where unidentifiable information becomes identifiable at some point in time. This, in turn, produces uncertainty around personal information similar to the 'expansionist' approach.

The same argument applies to the proposal made by Hon et al. to first minimise identification and then apply data processing rules proportionate to the risk[136]. As already noted above, developments in AI means that a subject could become identifiable or identified or be re-identified at any time. Therefore, in both proposals, the application of data processing rules proportionate to the risks results in different levels of protection for personal information. Indeed, Schwartz and Solove admit that

[130] Ibid.

[131] PM.Schwartz and DJ.Solove, 'The PII problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 N.Y.U. L. Rev. 1814, 1881

[132] Ibid 1814,1881.

[133] Ibid 1814, 1881.

[134] Ibid, 1880-1887.

[135] Ibid, 1879.

[136] Hon, Millard and Walden (n 129) 214-222, 227-228.

at its best, their approach produces different levels of safeguard for different categories of data.[137] Significantly, the proposal may be particularly complicated for new data protection regimes. For example, since the proposal will translate into applying different rules to different categories of personal information and even to the organisations processing the data, it can also create confusion and inconsistencies in the application of data processing principles.

## B. The Context of Harm

Gratton, [138] Cate[139] and Calo[140]offer alternative views based on the identification of an objective risk of harm. The authors argue that to establish that information is personal, it is useful to query the nature of harmful consequences arising from the use of such information. We further argue that it is equally important to determine whether such harmful consequences are the focus of data protection laws. In this respect, Calo distinguished between subjective and objective privacy harms. He conceived subjective privacy harm as an unwanted perception of observation. Subjective harm denotes the degree of antipathy which an individual feels towards being observed and may result in mental, emotional or psychological distress. This harm is subjective in the sense that it is internal to the person being harmed.[141] The critical requirement in subjective privacy harm is that observation is unwanted and to demonstrate this, Calo argues that when a person himself publicises the personal information or understands and agrees to its use, he does not invoke the sense of violation or harm. However, a person feels violated if the same information was collected by surreptitious means.[142] Conversely, objective privacy harm is the unanticipated or coerced use of information concerning a person against that person and to constitute objective privacy harm; information use must be unanticipated.[143] Hence the objective categories of privacy harm are, therefore, negative and external actions justified by reference to personal information. Examples include the unanticipated sale of a user's information that results in spam, or exploitation for crimes such as identity theft.[144] Cate appropriately associates the harmful consequences here not with the concept of individual control over personal information but with the need to protect individuals from uses of information which are unfair or harmful in a tangible or objective way.[145] Gratton similarly argues that the categorisation of information as personal must coincide with the ultimate purpose of data protection laws. As she observes, the legislative intent behind data protection laws is protecting the privacy of individuals from harmful consequences which may arise from organisational processing of personal information. This is the purposive rule of interpretation, which examines the aims of the drafters of law and the objectives underlying the legislation. Therefore, particular types of data handling activities must carry an underlying risk of harm, which is

[137] Schwartz and Solove (n 132) 1877.

[138] E Gratton, 'If Personal Information is Privacy Gatekeeper, then Risk of Harm is the Key: A Proposed Method for determining what Counts as Personal Information' (2013) 24(1) Alb LJ Sci &Tech 1.

[139] F H. Cate, 'The Failure of Fair Information Practice Principles', in Jane K Winn (ed) *Consumer Protection in the Age of the "Information Economy"* (Routledge, 2006) 341, 342.

[140] R Calo, 'The Boundaries of Privacy Harm' (2011) 86(1) Ind. L.J. 1.

[141] Calo (n 141) 1, 15.

[142] Ibid, 23.

[143] Ibid.

[144] Ibid 4 -15.

[145] Cate (n 140).

objective rather than subjective.[146] Being under surveillance or dignitary harm are examples of harm which could fall under the subjective category.[147] However, financial, economic or physical harm other than distress, would be objective harms, which are the proper concerns of data protection legislation. Gratton's examples include the theft of personal information from a bank which she argues can lead to objective harms such as fraud or identity theft.[148]

We can use an IP address as a specific example here. I may dislike the fact that my IP address could disclose my location because it locates my device connected to the internet, but the feeling of violation is in a subjective sense only. Therefore, if on the one hand, I feel violated by the collection or storage of my IP address, (which may be analogous to someone opening an address book and finding my home address in the case of static IP addresses), unless they come to my house (uninvited), I do not know that they know this address and may not feel threatened by that knowledge. However, even if I do, not everyone, and more importantly, not everyone everywhere feels threatened because other people know where they live and in the case of dynamic IP addresses, where they live temporarily. It is, therefore, a subjective risk and an issue for general privacy laws. In *Schrems*, the European Court had struck down the safe harbour agreement between the EU and the US. The agreement allowed data of EU origin to be transferred to self-certifying US companies on the basis that it raises a presumption of compliance with the adequate level of protection required under article 25 of the now-repealed EU Directive. However, in striking down the agreement, the court upheld the contention of the complainant, Mr Schrems who alleged that the US did not ensure an adequate level of protection of personal data held in its territory against surveillance activities by public authorities particularly the National Security Agency (NSA). Although the reference to Schrems here does not suggest endorsement of so-called 'snooping' by US law enforcement agencies, the case does underline the fact, noted earlier the article, that in the US and EU, there are different views about the interference of public authorities with private life and private communication.

On the other hand, in contrast to IP addresses, if my banking details are lost, stolen or accidentally disclosed by my bank, I could or may indeed have suffered financial losses. The harm, in this case, can be objectively determined as anyone in my position feels threatened in the same way. In criticising the *Schrems* judgement, for example, Determann correctly hinged his argument on the fact that the claimant 'could hardly show any plausible harm or need of protection'.[149] This form of harm is, therefore, properly the subject of data protection laws, and there is an emerging trend in this area with laws that emphasise the prevention of commercial exploitation of privacy. The APEC framework focuses on preventing harm to individuals from the wrongful collection and misuse of their information and incorporates a 'preventing harm' principle.[150] Also to underline the context of harm, the US Bill of Consumer Rights[151],

[146] Gratton (n 139) 45.

[147] Ibid, 47.

[148] Ibid, 68.

[149] L Determann, 'Adequacy of Data Protection in the USA: Myths and Facts' (2016) 6(3) International Data Privacy Law 244, 246.

[150] See e.g. Preamble to APEC Privacy Framework 2005; see also Principle 1.

[151] The White House, 'Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (February 2012)

a proposed Bill for online privacy, which was never passed by Congress, proposed a "respect for context" principle as a prerequisite to any processing. It provides that people 'have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.'[152] This recognition implies that if use must be consistent with a specific context, the harm would also be relative to context.

It is important to note that although it has not been canvassed in the context of the definition and scope of personal data, the risk-based approach is not new to EU law. For example, the WP29 asserts that it was well-known in relation to articles 17, 20 and 8 under the Directive and significantly promoted by articles 22,23, 28, 33 and 38 and 39 of the GDPR. Notably, the WP29 objected to the approach on the basis that it shifts the focus of regulation and compliance from data collection to data use and has the propensity to erode the fundamental right to protection of personal data guaranteed under article 8 of the Charter.[153] The main arguments against the fundamental right approach have been made above. In addition, Gellert has also opined that the right based and risk-based approaches to data protection are not diametrically opposed and should even be considered twins in the sense that both balance the harm and benefits associated with certain principles of data processing.[154] Furthermore, since the GDPR already contains provisions that significantly focus on risk management, attention should shift to developing frameworks for effective implementation (such as a comprehensive framework for identifying and mitigating privacy harm) that is presently lacking because, in privacy discourse, a consensus is still being developed around what constitutes harms.[155] This position reinforces the earlier assertion on the need for a clear concept of harm in the jurisprudence of data protection. In other words, if 'data protection and privacy laws are meant to protect people, not data', then it is important to determine what exactly are people being protected (from). 'What threats? What harms? What risks?'[156]

Finally, it is instructive to mention that GDPR itself alludes to the context of harm.[157] Article 35(1) provides, where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Under recital 75, such 'high risk' to the rights and freedoms of natural persons, may result from personal data processing which could lead to physical, *material or non-material damage,* in particular: *where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage* to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised

https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf accessed 09/02/2020.

[152] Ibid, 1.

[153] WP29, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks' (WP 218 30 May 2014) 2-3.

[154] R Gellert, 'We have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between Roghts-Based and the Risk-Based Approaches to Data Protection' (2016) 2 European Data Protection Law Review, 481, 491-492.

[155] F H. Cate, C Kuner, C Millard, Dan Jerker B Svantesson, and O Lynskey, 'Risk Management in Data Protection' (2015). Articles by Maurer Faculty 2628 h9p://www.repository.law.indiana.edu/facpub/2628 accessed 09/02/2020.

[156] Centre for information Policy and Leadership, (n 126) 2.

[157] See GDPR art. 33(1).

reversal of pseudonymisation, or any other significant economic or social disadvantage'. Although these provisions focus more on specific types of risky processing that is, "large-scale" processing, "systematic and extensive evaluation" and "systematic monitoring", the underlying rationale is that some types of personal processing carry more risk of harm than others. It is a recognition that not all processing is equally intrusive or harmful, and all personal data are not equally embarrassing, or sensitive or damaging. Depending on the context, personal data can be relatively harmless or extremely harmful, and it may relate to subjective harm suited for broader privacy laws or objective harm that falls within the ambit of data protection legislation.

Ultimately, the determination of information that constitutes personal data must rest on the answers to three broad questions. These are; what is the objective of the data protection law? What is the nature of the harm it proposes to address? Do these harms fit into the niche area of data protection, or does broader privacy legislation better address them? As a template, the definition of personal data would indicate that personal data can be any information that relates to an identified or identifiable natural person, but it must also be reasonably likely to cause harm in the context in which the processing takes place. Harm would be defined not by reference to subjective feelings of being hurt or discomfort, but regarding objective standards such as fear of theft, fraud, misuse or other compromises of the data.

## 5. Conclusion

The increasing adoption of EU data protection law is a seeming endorsement of the principles and concepts it embodies. Mostly its definition of personal data is accepted as correct, and many data protection regimes continue to borrow this definition. This article has explored the origins of the EU definition of personal data and linked it to the ideological underpinnings, history, experiences and the privacy jurisprudence of the EU. If alternative accounts of privacy are taken as correct; however, then the adoption of the EU concept of personal data cannot be taken as a consensus on the concept of privacy itself. As the article further demonstrated, even if the widespread adoption of the EU concept is justified on the grounds of trade or convenience, the expanding scope of personal data will become problematic as technology evolves. The alternative definition proposed is of a concept of personal data predicated on harm causing information.

There are compelling reasons why the context of harm-based approach should appeal to data protection regimes. Firstly, it shifts the focus of law and policymakers from the relative conceptions of privacy and helps to underline the primary objective at the heart of the regulation of data processing, that is the protection of individuals from the potentially harmful consequences of data processing. After identifying this objective, data protection regimes are able to distinguish subjective harm which is properly the subject matter of privacy laws and in respect of which general privacy laws (such as the constitution of respective countries) already exist, from objective and verifiable harm which should be the focus of data protection laws. In this way, the harm-based approach better articulates the construction of data protection as a social good and its objectives and functions as a consumer protection mechanism.

Secondly, a harm-based approach is consistent with the need to strike the right balance between the protection of personal data and the promotion of innovation in new technologies. For developing countries which stand to gain from the social benefits such as improved medical diagnosis and healthcare services offered by new technologies, there is more pressure to converge around the concept of harm causing personal data, rather than the EU expansionist approach which could potentially inhibit information collection by designating any information personal data. The overall advantage of the harm-based approach here is that for emerging data protection regimes, it presents a pragmatic basis for assessing the extent to which it reasonable to trade social benefits for individual and often marginal privacy gains.