Spring Issue 2023

AMSTERDAM LAW FORUM

The International Law Journal of Vrije Universiteit Amsterdam

Volume 15 Issue 2

COMMENTARY ARTICLE

EXPLORING THE TENABILITY OF THE GDPR BECOMING THE 'LAW OF EVERYTHING'

Hacel Grace T. Dela Cruz *

I. Introduction

The 1957 launch of Sputnik occasioned in philosopher Hannah Arendt a line of inquiry about technology and its effects to human existence.[1] Thus in *The Human Condition*, Arendt offered a proposition: "a reconsideration of the human condition from the vantage point of our newest experiences and our most recent fears."[2] As if in assent, Nadezhda Purtova's *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*[3] reexamined the future of society from the vantage point of a singular source of fear: what she perceived to be the unimpeded expansion of the legal notion of "personal data". This expansion of "personal data", Purtova posits, is inevitable. But is it?

This article reconsiders Purtova's theory of the "Law of Everything" in which she posits that in the near future, everything will be "information" and all "information" will be "personal data"; hence, data protection laws will become the law of "everything". This article argues that while the legal notion of "personal data" is broad, it is not limitless. Personal data is inherently contextual and as such, every instance of the legal inquiry—"is this considered processing of personal data under the GDPR?"—is reined in and limited by the context in which personal data exists. This context-based analysis forestalls data protection laws from being the law of "everything".

II. The Onlife World

Philosopher Luciano Floridi coined the term "onlife" to refer to a "new experience of a hyperconnected reality" in which all human experiences are mediated by and interwoven with information and communication technologies (ICTs).[4] In this onlife world, the environment is so pervaded by information flows and processes that it becomes insensible to ask whether one may be online or offline.[5]

---

* *Hacel Grace T. Dela Cruz, 2023 LL.M. Candidate of International Technology Law, Vrije Universiteit Amsterdam.*

[1] Hannah Arendt, *The Human Condition* (The University of Chicago Press 1998), p. 5.

[2] Ibid.

[3] Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) Law Innov. Technol.< https://doi-org.vu-nl.idm.oclc.org/10.1080/17579961.2018.1452176> accessed 18 December 2022.

[4] Luciano Floridi, "The Onlife Initiative" in Luciano Floridi (ed), *The Onlife Manifesto: Being Human in a Hyperconnected Era* (Springer 2015), p. 12.

[5] Idem, p. 1.

Floridi and colleagues used the onlife world as a model to explore how the pervasiveness of ICTs is radically changing the human condition.[6] But for Purtova, the onlife world is not simply a model; it is humanity's destiny.[7]

In this onlife world, everything is information and all information is "personal data".[8] This scenario will be brought about by two forces: *first* is the full realization of the onlife world (technology); and *second,* is the broad definition of "personal data" (law).[9]

II.1 First Driving Force: Technology

As to the *first*, Purtova thinks that while the "onlife world of total connectivity and data-driven agency" has not arrived, it is firmly on its way.[10] As an indicator of this inevitability, Purtova points to the ubiquitousness of smart technologies which, she observes, is no longer confined to small devices but is now increasingly being used in homes (i.e. smart homes) and cities (i.e. smart cities).[11] She foresees that in the future, all environments will be "smart" and therefore, the environment and its people will be "datified"—that is, transformed into data and information.[12] Purtova's vision is very much reminiscent of Mireille Hildebrandt's world of "data-driven agency" where artificial intelligence is capable not only of perceiving its environment but of acting upon it based on the massive amounts of data it processes.[13]

II.2 Second Driving Force: The Law

Unlike the technological nature of the *first* driving force, the *second* is of a legal nature. Purtova argues that the legal notion of "personal data" is broad and undefined.[14] Article 4(1) of the General Data Protection Regulation defines "personal data" as "any information relating to an identified or identifiable natural person...". To constitute "personal data", an "information" must satisfy two tests: *first*, it must relate to a natural person; and, *second*, that natural person must be identifiable from that information.[15] These two tests will hereinafter be referred to as the "relationality test" and the "identifiability test", respectively.

Purtova insists that these two tests cannot rein in the expanding scope of "personal data". Anent the relationality test, Purtova notes that the Court of Justice of the European Union's decision in *Nowak*

[6] Idem, p. 7.
[7] Purtova 2018, supra note 3, p. 78.
[8] Idem, p. 42.
[9] Idem, pp. 42-43.
[10] Idem, p. 73.
[11] Idem, p. 56.
[12] Idem, p. 41.
[13] Mireille Hildrebrandt, 'Law as Information in the Era of Data-Driven Agency' (2016) Mod. Law Rev. <http://www.law.nyu.edu/sites/default/files/upload_documents/Hildebrandt-Law%20as%20Information%20in%20the%20Era%20of%20Data-Driven%20Agency.pdf> accessed 18 December 2022, p. 4.
[14] Purtova 2018, supra note 3, p. 48.
[15] Benjamin Wong, 'Delimiting the Concept of Personal Data after the GDPR' (2019) Leg Stud. <doi: 10.1017/1st.2018.52> accessed 18 December 2022, p. 519.

vs. Data Protection Commissioner[16] has given imprimatur to a wide interpretation of the qualifier "relate to". In *Nowak*, the CJEU ruled that the relationality test is passed if "the information, by reason of its *content, purpose or effect,* is linked to a particular person."[17] Purtova observes that these three conditions are alternative and not cumulative, and thus, the scope of "personal data" grows even broader.[18] Hence, in the same manner that data can "relate to" an individual merely by its content (e.g. name, address), data can also "relate to" an individual regardless of content but because of the purpose for which it is processed (e.g. to influence the individual).[19] In this sense, even information traditionally not seen as personal data (e.g. weather) is "personal data" when used with a purpose involving a natural person.[20]

On the other hand, the identifiability test requires that the natural person to which the information relates must be either already identified or identifiable.[21] On this note, Recital 26 of the GDPR states that "to determine whether a person is identifiable, account should be taken of all the *means likely reasonably* to be used either by the controller or by any other person to identify the said person…"[22] Purtova opines that what counts as "likely reasonable" means of identifiability is very broad.[23] She cites *Breyer v Bundesrepublik Deutschland*[24] in which the CJEU took note of only the legal means available to the controller to determine what is "likely reasonable" means of identifiability.[25] From this, Purtova surmises that as far as case law goes, the only instance when the means are not considered "likely reasonable" is when they are illegal.[26]

III. Law of Everything: A Closer Look

Purtova's analysis culminates in a theory of "Law of Everything"— that is, given the (i) broad scope of the legal notion of "personal data", and the (ii) inevitable arrival of the onlife world where everything is datified, everything will constitute information and all information will be "personal data". Purtova predicts that chaos will ensue because a law that attempts to govern everything is not scalable and will end up governing nothing. For Purtova, a "system overload" scenario is bound to happen: when everything is personal data and everything triggers personal data protection, the already high-intensive data protection compliance under the GDPR becomes non-scalable and the rights and obligations derived from it become simply impossible to implement in a meaningful way.[27] As fascinating as this theory sounds, it is not without flaws.

A closer analysis reveals that the "Law of Everything" rests on a singular assumption: that personal data exists in a vacuum. Indeed, it is only by assuming that personal data exists unaffected by other

[16] Case C-434/16 *Nowak vs. Data Protection Commissioner* [2017] ECLI:EU:C:2017:994
[17] Ibid, para. 35. Italics supplied.
[18] Purtova 2018, supra note 3, p. 54.
[19] Ibid.
[20] Idem, pp. 57-59.
[21] General Data Protection Regulation, art. 4(1).
[22] Italics supplied.
[23] Purtova 2018, supra note 3, p. 65.
[24] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779.
[25] Ibid, para. 49.
[26] Purtova 2018, supra note 3, p. 65.
[27] Ibid, p. 75.

factors that it becomes possible to hypothesize that it has one — and only one — unavoidable end (i.e. to be "everything"). But this is not the case. On the contrary, personal data is inherently contextual.

III.1 Personal Data and Processing are Contextual

To begin with, even the GDPR does not apply to personal data in a vacuum, but to its processing.[28] Article 2(1) of the GDPR expressly states: "[t]his Regulation applies to the *processing* of personal data wholly or partly..."[29] Implicitly, this means that the question "is this personal data?" yields a different response than "is this a processing of personal data?". In contrast to the *former,* the *latter* is a two-level inquiry that specifically targets the applicability of data protection laws. Unfortunately, Purtova's analysis is focused only on the *former* and, by answering in the affirmative, already jumps to the conclusion that GDPR must apply. The analysis entirely missed the *latter* question which, ironically, was *the* analytical entry point to exploring the actual tenability of whether "everything" can be subjected to data protection laws.

That personal data exists in the context of processing implies that personal data is contextual. At any given time, data exists in a "data environment".[30] Coined by Mark Elliot and colleagues, "data environment" refers to "the set of all possible data that might be linked to a given dataset."[31]

Moreover, data in any data environment has a lifecycle: creation, collection, processing, re-shaping, aggregation, storing, and deletion.[32] An implication of this is when data relates to a natural person by reason of content, it is likely to remain as "personal data" throughout its lifecycle.[33] However, when data relates to a natural person by reason of its purpose or effect, it is "personal data" only for a specific segment of its lifecycle and only as long as its purpose or effect relates to a natural person.[34] On this point, Dalla Corte offers a good illustration: a passport number, which relates to a natural person by virtue of content, will remain "personal data" throughout its lifecycle.[35] On the contrary, details about a vehicle will relate to a natural person only by virtue of purpose or effect such as, for instance, in the context of driver performance evaluation.[36] Once this purpose or effect ceases and the data exists in a data environment without other data relating it to a natural person, it ceases to be "personal data" at that stage of its lifecycle.

---

[28] Lorenzo Dalla Corte, 'Scoping Personal Data: Towards a Nuanced Interpretaton of the Material Scope of EU Data Protecton Law' (2019) EJLT <https://ejlt.org/index.php/ejlt/article/view/672/908> accessed 18 December 2022, pt 4.1.
[29] Italics supplied.
[30] Mark Elliot et al., 'Functional anonymization: Personal data and the data environment' (2018) CLSR, <https://doi.org/10.1016/j.clsr.2018.02.001> accessed 18 December 2022, p. 213.
[31] Ibid.
[32] Elliot 2018, supra note 29, pt 4.2.1; see also Meg Leta Ambrose, 'It's about time: privacy, information life cycles, and the right to be forgotten' (2013) Stanford Technol Law Rev < http://stlr.stanford.edu/pdf/mostlitigatedpatents.pdf> accessed 7 April 2023.
[33] Ibid.
[34] Ibid.
[35] Ibid.
[36] Ibid.

Taking these into consideration, Purtova's absolutist argument about weather constituting personal data in the onlife world becomes more nuanced: inside or outside the onlife world, weather may indeed be personal data when it relates to a natural person by purpose or effect. But once the data moves throughout its lifecycle (e.g. when it is cleaned or aggregated)[37] and into a data environment barren of other data with which it can be linked together to relate to a natural person, weather ceases to be personal. At that stage, even when weather is processed, its processing shall not fall under the GDPR because it has, in the meantime, ceased to be personal.

III.2. Identifiability is Contextual

Because personal data exists in a data environment and undergoes a lifecyle, each instance of processing adds a layer of context that is bound to be considered in determining whether data is personal.[38] Therefore, analyzing whether data is personal is not as linear as what Purtova suggests it to be. In fact, the identifiability test's standard of "likely reasonable means of identifiability" supports a more complex framework of analysis. Indeed, whether the considered means of identifiability are "likely reasonable" requires a case-to-case analysis that must consider the relevant factors attending the specific case.[39] Stated differently, contrary to Purtova's reading of *Breyer*,[40] the "likely reasonable means of identifiability" standard does not contemplate absolutely all legal means imaginable but only what is reasonable, likely, and relevant to the case. Hence, ultimately, identifiability is contextual: at any point, and depending on the context, data may be personal at one moment, and anonymous in another.[41]

IV. Conclusion

In a way, "personal data" is to Purtova what Sputnik meant to Arendt: it raised in her an urgency to examine the order of the society as it relates to data protection. Yet, the fallacy of the "Law of Everything" is in conflating "broad" with "limitless". What is broad is not necessarily limitless. For, while certainly European lawmakers intended "personal data" to have a wide scope,[42] its reach is not without bounds. Personal data invariably exists in a data environment and, as such, its processing exists in a context. The contextual elements in which personal data and its processing exist constitute the limiting framework through which the legal inquiries "is this personal data?" and "is this a processing of personal data?" are analyzed. From this vantage point, while the online world may arrive and everything might become information, not everything will be "personal data" and not every "processing" will be subject to the GDPR.

[37] Dalla Corte 2019, supra note 25, pt 3.2.
[38] Idem, pt 4.1.
[39] Idem, pt 4.3.1.
[40] *Patrick Breyer* (n 23).
[41] Christopher Millard & W Kuan Hon 'Defining 'Personal Data' in e-Social Science' (2011) Inf. Commun. Soc. <https://www.tandfonline.com/doi/abs/10.1080/1369118X.2011.616518> accessed 18 December 2022, p. 4.
[42] Article 29 Data Protection Working Party adopting Opinion 4/2007 on the concept of personal data, p. 4.