Why accuracy needs further exploration in data protection

Elisabetta Biasin

{Elisabetta.biasin@kuleuven.be}

KU Leuven Centre for IT & IP Law, Belgium

Abstract. Accuracy, understood as a principle of data protection law (Art 5(d) GDPR), has received timid attention in EU legal scholarship so far. This short paper suggests why accuracy deserves more attention in data protection studies, having regard to its conceptualisation, its role as a principle of data processing in the GDPR and the other principles of data processing, and the possible risks of data subjects' misrepresentation and discrimination.

Keywords: Accuracy, GDPR, data protection, AI.

1 Introduction

Overview and article structure – Accuracy is a principle of data protection legislation requiring the processing of personal data to be accurate and kept up to date. In case of personal data inaccuracy or errors, data protection legislation provides the right to data subjects to obtain rectification under certain conditions. In the last years, discussions about possible bias and errors in data and their processing involving the use of Artificial Intelligence (AI) fostered a debate on the potential risks of misrepresentation and discrimination for data subjects. Starting from these elements, this short paper calls for more exploration of the accuracy principle in data protection. To do so, the paper proposes an initial investigation of the literature state-of-the-art concerning the accuracy principle in data protection (section 2) and highlights possible gaps (section 2.2). Section 3 presents a case study to underscore the relevance of accuracy for AI-based processes in a specific field, i.e. personalised medicine. Section 4 offers conclusions on how to which future research could tackle the challenges identified so far.

2 Accuracy

2.1 Accuracy in data protection law

Overview – In data protection law, the notion of accuracy has been present in the national, international and European regulatory instruments since the last quarter of the 1900s. At a national level, the first pertinent references date even back to the 1974 US Privacy Act. This act required the covered agencies to maintain all records "with such accuracy, relevance, timeliness, and completeness as [it was] reasonably necessary to assure fairness to the individual in the

CAIP 2021, November 20-24, Bologna, Italy

DOI 10.4108/eai.20-11-2021.2314205

determination" (5 USC, §552a(e)(5)). At a supranational level, accuracy appeared first in the Organisation for Economic Co-operation and Development (OECD)'s Privacy Principles. In particular, the data quality principle required that "[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date" (OECD, 1980). In 1981, Convention 108 foresaw that personal data undergoing automatic processing "shall be accurate, and when necessary, up to date". In the EU, the accuracy principle appeared in the 1995 Data Protection Directive (DPD). It was foreseen under the so-called 'principles relating to data quality' (Article 6(1)(d) DPD), which became – later on in the General Data Protection Regulation (GDPR) – the 'principles relating to processing of personal data' (Article 5 GDPR).

What is accuracy? – Neither the abovementioned international instruments nor EU law provisions define 'accuracy'. The GDPR itself does not contain a definition of it. The GDPR only implies that data shall be "accurate and, where necessary, kept up to date" (Article 5(1)(d) GDPR). "[E]very reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (id.). Further to that, a few other minor references in the GDPR concern accuracy. Accuracy is mentioned in relation to data subjects' rights – especially the right to rectification (Article 16 GDPR) and the right to restriction of processing (Article 18 GDPR).

2.2 Literature state of the art and core problems

Is it a self-explanatory concept? – Accuracy and its elaboration as a concept seem not to have been particularly addressed in EU legal studies [1]. Some have observed that the principle of accuracy would be a 'crocodile of data protection' [2] for its antiquity. As the crocodile in the animal kingdom, the principle saw few content-related changes over its evolution in data protection law (id.). Even despite the significance and track record of the principle in data protection law, neither courts nor scholars have felt it necessary to spend much time or ink elaborating the content of the principle (id.). The United Kingdom's Supervisory Authority Information Commissioner's Office (ICO) maintained that accuracy is a sort of self-explanatory concept, as it 'is usually more obvious whether personal data is accurate' [3].

What is the role of accuracy in the GDPR? – According to Hallinan and Borgesius [1], the principle of accuracy plays a double role in the structure GDPR. First, it is a substantive norm requiring personal data to be accurate, and where necessary, up to date (Article 5(1)(d) GDPR). Second, the "accuracy principle functions as instrumental of other data protection principles and as an applicability criterion for data subjects' rights" [2] – such as the right to rectify inaccurate personal data and the right to object to the processing of inaccurate personal data (Dimitrova [1] in this regard, wrote about 'accuracy as an enabler of the right to rectification').

Accuracy and the other data processing principles: "unacknowledged trade-offs"? – Some scholars have underlined an unclear interaction between the accuracy principle itself, the other data processing principles, and the data subjects' rights. In Finck's and Biega's opinion [4], there are unacknowledged trade-offs between data protection principles. Accuracy and fairness, for example, are seen most in tension with the data minimisation principle (id.). In this respect, the authors called for more engagement from multiple disciplines in the years to come, "to establish normatively, legally, and technically how to balance data minimisation with other

GDPR requirements" – such as fairness and accuracy – which might be at odds with the minimisation principle (id., p. 40). Therefore, not only the principle should be investigated as such on its own, but also in its relation with the other principles of data processing.

On the applicability of the accuracy to inferences and (medical) opinions – The applicability of accuracy to personal data seems to be undiscussed. But more is discussed about the applicability of the accuracy principle to the inferences (including profiling) based upon personal data. Authors distinguish between factual and non-factual data [1] [6] or 'factual data' and 'predictive data'). Hallinan and Borgesius [2] argue that 'personal data opinions' should be considered as personal data to which accuracy requirements would apply (contra: [24]). Moreover, if accuracy applies to opinions relating to an individual, human-generated opinions by medical professionals should be considered as such [25] – and hypothetically, enforcing data subjects' rights (including the right to access and rectify medical opinions), should be possible for such opinions. However, it appears that further research would be needed for the applicability of these rights to medical opinions, as well as to the likely different manifestations of these rights in EU jurisdictions[2].

Between low- and over-accuracy – According to Article 5(1)(d) GDPR, accuracy requires to have "regard to the purposes for which [data] are processed". As Dimitrova puts it [1], accuracy is purpose and context-dependent. "[D]ata needs to be accurate enough for the specified purpose of the processing" (id.). On the one hand, the purpose of the processing is crucial to avoid any adverse effects caused by a low level of accuracy in processing activities.[1] On the other hand, however, data should not be more accurate than what is required by the purpose of the processing [5]. In fact, while it might seem obvious that a lack of accuracy may bring disadvantages for individuals, paradoxically, also a high degree of accuracy may bring its shortcomings. According to Chen [6], enhanced accuracy (or 'over-accuracy') may bring forth a range of disadvantages, including new forms of discrimination and the loss of individual manoeuvre space (id.). [2]

Risk caused by errors or inaccurate data and the related inferences may cause unfair discrimination (see WP29 [8], a contrario). In literature, research studying possible interrelations between data protection and non-discrimination law has increased in recent years (e.g. Binns [10]; Gerards & Borgesius [11] – to name the most recent ones). However, some deem the interrelationship between the GDPR and EU non-discrimination laws deserve further

[1] We could make the following example: Inaccurate risk profiles resulting from automated analyses in the field of public security. In that context, false-positives could result in investigating and even arresting innocent people. False-negatives could result in criminals being out of scope (see Vedder & Custers, [7] p. 27)

[2] Example: certain groups of people, labelled with a combination of demographic, socio-economic or behavioural indicators, are considered, for example, less creditworthy or employable. The conclusion by a scoring system, for instance, that 'those who live in a particular neighbourhood, loyal to certain brands and without a college degree are more likely to default on a loan', can be legal as it is not based on any categories prohibited by anti-discrimination law. Even if these groups of individuals may not pertain to certain protected groups, they may indeed be disadvantaged for reasons they have little control over, and they might be treated as inferior in one particular context (example from Chen [6]).

study [11]. Furtherance of these studies could help understand the interaction between these instruments – including accuracy – to ultimately help protecting against algorithmic discrimination.

On privacy, informational self-determination and misrepresentation – Finally, it its Opinion on purpose limitation, the EU body Article 29 Working Group (WP29) included inaccuracy and discrimination amongst the risks and challenges posed by big data to the right to personal data and privacy. Also, Hallinan and Borgesius [2] identified the misrepresentation of the data subject as a risk caused by inaccuracy to the fundamental right to privacy and data protection. In its first role of ensuring personal data to be accurate and be kept up to date, the principle aims to ensure "that the individual to whom personal data relate is not subject to misrepresentation, and the consequences of misrepresentation, through their personal data" (id., p. 3). Further, if personal data relating to an individual are not accurate, it may even impact individuals' identity and constitute an interference with the right to respect for private life. They base their arguments on the Romet v the Netherlands case (where the European Court of Human Rights (ECtHR) found a lack of action to correct inaccurate identity information as an interference to the right to privacy). The interplay of these risks posed to the right to privacy with the meaning and consequences of misrepresentation are worth exploring further – also having regard to individuals' informational self-determination.

2.3 A case study: accuracy in personalised healthcare

For a conception of accuracy in healthcare – A particular field in which accuracy is increasingly critical is healthcare. Over the last decades, modern healthcare systems have undergone a radical change towards personalised healthcare [12] [13]. Artificial Intelligence (AI) in healthcare is growingly used for its predictive functions, as it is deemed to have the potential to, amongst others, enhance clinical decision-making and facilitate disease diagnosis. [14]. In specific fields notably (e.g. image-based diagnosis), technology seems to have reached 'expert-level diagnostic accuracies' – and in some cases, performing even more reliably than human experts (id.).

Accuracy in healthcare – In data protection law, if data used in profiling and automated decision making is inaccurate, any resultant decision or profile will be flawed. Decisions may be made on the basis of outdated data or the incorrect interpretation of external data. Moreover, it might lead to inappropriate predictions or statements about someone's health [8]. Adjusting inaccuracies of personal data or minimising risks of errors may prevent such discriminatory effects on natural persons – including in healthcare. In this regard, recent studies have shown that predictive algorithms based on large data sets may lead to direct discrimination, indirect discrimination, or disparate mistreatment of certain groups [9]. Bias and errors and so inaccuracies in data sets may enhance the risks of unfair discrimination amongst individuals or groups [15] [16] [17].[3]In healthcare, unfair discriminatory processes may result in health inequalities across and within countries [17] [18].

[3] It might be useful to clarify that this does not mean that having accurate data sets would eliminate the risks of unfair discrimination for individuals or groups. However, the level of accuracy may play a role in enhancing such risks.

Examples of pitfalls in personalised healthcare – Research has shown that the use of automated processing in personalised healthcare comes with challenges [19]. To bring some examples, in 2019, a group of researchers showed that a widely used algorithm in healthcare and affecting a large number of patients exhibited 'significant racial bias' [20] [21]. In another case, Zou and Schiebinger [21] underscored how acclaimed research for detecting skin cancer through a deep neural network (by Esteva et al., [22]) resulted from biased data sets due to its limited test on a specific part of the population [21]. The World Health Organisation recently validated these concerns in a recent study [23]. The study explains how not only databases and machine-learning training sets might be biased, but also algorithms. Bias could lead to the allocation of resources discriminating, e.g. against people of colour; or, decisions related to gender, ethnicity or socio-economic status might similarly be biased (id., p. 49). This situation could bring further health inequalities, resulting in the allocation of most resources to healthy people to keep them healthy rather than to a disadvantaged population (id.).

3. Conclusion and future avenues for research

The above considerations have briefly illustrated some of the encountered gaps concerning the study of accuracy and its role in data protection. Furthermore, if applied in concrete situations – such as the case of personalised medicine – the principle may play a role vis-à-vis misrepresentation and discrimination and the risk of health inequalities. The current studies concerning accuracy seem to fail in providing a broad analysis of the accuracy principle. Avenues for scholarly research could address the following points:

(1) Re-consider the conceptualisation of accuracy as a principle of data processing on its own.
(2) Analyse the accuracy principle's role in relation to other principles of data processing and the data subjects rights.
(3) Scrutinise the role of the accuracy principle vis-à-vis the potential risks of misrepresentation and unfair discrimination.

References

[1] Dimitrova, D. (2021). The Rise of the Personal Data Quality Principle. Is it Legal and Does it Have an Impact on the Right to Rectification? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3790602

[2] Hallinan, D., & Borgesius, F. Z. (2020). Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle. International Data Privacy Law, 10(1), 10. https://doi.org/doi.org/10.1093/idpl/ipz025

[3] ICO. (2021, January 1). Principle (d): Accuracy. ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

[4] Finck, M., & Biega, A. (2021). Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3749078

[5] Fuster, G. G. (2010). Inaccuracy as a privacy-enhancing tool. Ethics and Information Technology, 12(1), 87–95. https://doi.org/10.1007/s10676-009-9212-z

[6] Chen, J. (2018). The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle. European Data Protection Law Review, 4(1), 36–52. https://doi.org/10.21552/edpl/2018/1/7

[7] Vedder, A., & Custers, B. (2009). Whose responsibility is it anyway? Dealing with the consequences of new technologies. In Evaluating new technologies. Methodological problems for the ethical assessment of technology developments (Vol. 3, pp. 21–34). Springer.

[8] WP29. (2017). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

[9] Loi, M., & Christen, M. (2021). Choosing how to discriminate: Navigating ethical trade-offs in fair algorithmic design for the insurance sector. Philosophy & Technolocy, 26. https://doi.org/10.1007/s13347-021-00444-9

[10] Binns, R., & Kirkham, R. (forthcoming, 2021). How Could Equality and Data Protection Law Shape AI Fairness for People with Disabilities? ArXiv: https://arxiv.org/abs/2107.05704

[11] Gerards, J., & Zuiderveen Borgesius, F. (2020). Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3723873

[12] Verhenneman, G. (2020). The patient's right to privacy and autonomy against a changing healthcare model. KU Leuven. Faculteit Rechtsgeleerdheid.

[13] Hood, L., & Friend, S. H. (2011). Predictive, personalised, preventive, participatory (P4) cancer medicine. Nature Reviews Clinical Oncology, 8(3), 184–187. https://doi.org/10.1038/nrclinonc.2010.227

[14] Yu, K.-H., Beam, A. L., & Kohane, I. S. (2018). Artificial intelligence in healthcare. Nature Biomedical Engineering, 2(10), 719–731. https://doi.org/10.1038/s41551-018-0305-z

[15] Vedder, A., & Naudts, L. (2017). Accountability for the use of algorithms in a big data environment. International Review of Law, Computers & Technology, 31(2), 206–224. https://doi.org/10.1080/13600869.2017.1298547

[16] Mittelstadt, B. D. et al. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 205395171667967. https://doi.org/10.1177/2053951716679679

[17] Schoenberger, D. (2019). Artificial intelligence in healthcare: A critical analysis of the legal and ethical implications. International Journal of Law and Information Technology, 27, 171–203. https://doi.org/10.1093/ijlit/eaz004

[18] Ghassemi, M. et al. (2020). A Review of Challenges and Opportunities in Machine Learning for Health. AMIA Join Summits on Translational Science Proceedings. AMIA Joint Summits on Translational Science, 191–200

[19] Hoffman, S., & Podgurski, A. (2020). Artificial Intelligence and Discrimination in Health Care. 50.

[20] Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations.

[21] Zou, J., & Schiebinger, L. (2018). AI can be sexist and racist—It's time to make it fair. Nature, 559(7714), 324–326. https://doi.org/10.1038/d41586-018-05707-8

[22] Esteva, A., et al., (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118. https://doi.org/10.1038/nature21056

[23] World Health Organisation. (2021). Ethics and governance of artificial intelligence for health. WHO governance.

[24] Data Protection Commission. (2020, 01). Opinions—Everyone's got one, but does data protection law apply to them? Data Protection Commission. https://www.dataprotection.ie/dpc-guidance/blogs/opinions-everyones-got-one-does-data-protection-law-apply-them.

[25] Jove, D. (2019). Peter Nowak v Data Protection Commissioner: European Data Protection Law Review, 5(2), 175–183. https://doi.org/10.21552/edpl/2019/2/7.