Ethical Dimensions of the GDPR, AI Regulation, and Beyond[1]

HIELKE HIJMANS[I]

[I] Vrije Universiteit Brussels. Bruxelas, Bélgica.

CHARLES RAAB[2, II]

[II] University of Edinburgh. Edimburgo, Reino Unido.

ABSTRACT: Our digital society is changing rapidly, with emerging new technologies such as artificial intelligence (AI) and machine learning, robotics, and the internet of things. These changes trigger new fundamental ethical questions[3] relating to privacy, data protection and other values, including human rights and the way they are affected by the extensive and intensive use of data for analytical and practical innovations. This article explores these ethical dimensions and the extent to which the European Union's General Data Protection Regulation[4] (GDPR) of 2018 takes ethics into account in relation to these socio-technical developments. More briefly, it looks similarly but more selectively at the EU's proposed AI Act of 2021, which aims to regulate AI in relation to levels of risk[5]. It concludes with some observations on desirable institutional arrangements for making and applying ethical judgements in the regulation of advanced technologies that use personal data.

KEYWORDS: Privacy; ethics; GDPR.

1 An earlier version of this paper, "Ethical Dimensions of the GDPR" (2018) was prepared for inclusion in Cole, M. and Boehm, F. (eds.) (forthcoming) *Commentary on the General Data Protection Regulation*, Cheltenham: Edward Elgar. We are grateful to the editors for permission to use this material in a revised form.

2 Orcid: https://orcid.org/0000-0002-4579-0320.

3 Floridi calls this Information Ethics; the ethical impact of ICT on humans and society: Floridi, L. (2013), *The Ethics of Information*. Oxford: Oxford University Press.

4 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), OJ L 119/1.

5 Proposal from the European Commission for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts, COM/2021/206 final.

1 INTRODUCTION

The GDPR gives effect to the fundamental right to data protection. It is a major landmark in the development of data protection, with a global reach far beyond the European Union. The extent to which, and the way in which, it embodies and promotes adherence to ethical norms and values beyond mere legal compliance sends important signals to those who process personal data in all domains of the public and private sectors. The GDPR also sets rules aiming at the protection of fundamental rights more generally[6], and is meant to be future-proof. An important perspective of the GDPR is that it recognises the contribution of technology to economic and social progress[7], but holds that technology should be developed in a responsible manner and, in particular, that individuals should have control over their personal data. Moreover, in recent years ethical issues have been increasingly recognised in the data protection community and in "data-driven" innovation and implementation[8]. The initiative of the European Data Protection Supervisor (EDPS), starting with an opinion on digital ethics and the establishment of an Ethics Advisory Group[9], is just one illustration of the wider "turn" to ethics; further examples will be mentioned later.

2 ETHICAL DIMENSIONS OF PRIVACY AND DATA PROTECTION

Ethical considerations are part of the GDPR, but they are sometimes hidden in its Articles. The GDPR has elements of principles-based regulation, and is not just rules-based[10]. We explore how the GDPR encourages ethical judgements, starting from the notion that the processing of personal data should be designed to serve mankind[11]. Ethical notions about good and bad behaviour lie behind legal stipulations of what must, can or cannot be done.

6 Recital 4.

7 *E.g.*, Recitals 2 and 6. This recognition is foregrounded even more in the AI Act proposal.

8 Some authors question the seriousness and sincerity of attempts to put ethical values into practice. See *e.g.*, references in Raab, C. (2020), "Information Privacy, Impact Assessment, and the Place of Ethics", *Computer Law and Security Review*, 37, July, https://authors.elsevier.com/sd/article/S0267-3649(20)30009-1.

9 See https://edps.europa.eu/data-protection/our-work/ethics_en; European Data Protection Supervisor, Opinion 4/2015 of 11 September 2015, "Towards a new digital ethics"; Press Release EDPS of 28 January 2016, https://edps.europa.eu/data-protection/our-work/subjects/ethics_en.

10 See Black, J. (2008) "Forms and Paradoxes of Principles Based Regulation", LSE Legal Studies Working Paper No.13/2008; Raab, C. (2012) "Regulating Surveillance: The Importance of Principles", p. 377-385 in Ball, K., Haggerty, K. and Lyon, D. (eds.), *Routledge Handbook of Surveillance Studies*, London: Routledge; Raab, C. (2017) "Information Privacy: Ethics and Accountability", p. 335-347 in Brand, C., Heesen, J., Kröber, B., Müller, U. and Potthast, T. (eds.), *Ethik in den Kulturen – Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn*, Tübingen: Narr Francke Attempto.

11 Recital 4.

Data protection laws are no different in this respect, in that they are based on ethical notions that underpin the fundamental rights of privacy and data protection. What the GDPR – as well as earlier generations of data protection laws – lays down in legislation incorporates ethical principles, although their prominence, explicitness and clarity is intermittent and fragmentary across the various Recitals and Articles. Moreover, the range of ethical principles and human rights upon which the GDPR could have drawn is wider.

Ethical values are often expressed in vague language and slogans that have only moral force, yet they may overlap with sometimes enforceable rights. The Charter of Fundamental Rights of the European Union[12] ("Charter") establishes (an undefined) "human dignity" as a bedrock in Article 1, saying: "Human dignity is inviolable. It must be respected and protected". Dignity is also emphasised with regard to the elderly (Article 25) and workers (Article 31). Dignity is also a key value underlying privacy and data protection. For the EDPS, human dignity was the main driver for dealing explicitly with ethics: it envisaged inserting this ethical claim into the "ecosystem" of data protection[13]. However, "dignity" is only mentioned once in the GDPR – in Article 88(2), concerning processing in the context of employment. Elsewhere in the GDPR, Recital 4 contains a very general ethical reference, saying: "The processing of personal data should be designed to serve mankind". On the other hand, the GDPR's emphasis on respect for the "fundamental rights and freedoms" of natural persons is ubiquitous, and the GDPR specifies the fundamental right of data protection in a number of detailed rights of the data subject that have legal effect[14]. The notion of fairness plays a key role in this respect. Fairness is an ethical dimension that is central to legal requirements for data protection under international and EU law, as well as national law. Article 8 Charter requires fair processing, whilst Article 5(1)(a)) GDPR elaborates this and associates it with transparency, although it can be debated whether transparency is an element of fairness or a separate requirement. In any case, "fairness" is a highly complex and ambiguous concept[15] and its relationship to other principles can be seen in various ways. We will touch upon fairness again later on.

12 Official Journal of the European Union, C/303/1.

13 European Data Protection Supervisor, Opinion 4/2015 of 11 September 2015, *Towards a new digital ethics: Data, dignity and technology*; EDPS Ethics Advisory Group Report, *Towards a Digital Ethics*, 2018, available on edps.europa.eu.

14 GDPR Chapter III.

15 Clifford, D. and Ausloos, J. (2018) "Data Protection and the Role of Fairness", *Yearbook of European Law,* 37,1: 130-187.

Another, more general, precept is respect for the rule of law, reflecting the ethical and legal roots of the EU and its Member States. Respect for the rule of law is reflected in data protection laws by providing that the processing of personal data must always rely on a legal ground (Article 8 Charter and Article 6 GDPR). The GDPR incorporates traditional data protection principles established in landmark documents, such as the Privacy Principles of the Organisation for Economic Co-operation and Development (OECD) of 1980[16] and the Council of Europe Convention No. 108 of 1981[17] that underlie Data Protection Directive 95/46 (the Directive) and national laws. These principles require that personal data should be fairly and lawfully collected for a valid purpose; accurate, relevant, and up-to date; not excessive in relation to its purpose; not retained for longer than needed for the purpose; collected with the knowledge and consent of the individual or otherwise on a legal basis; not communicated to third parties except under specified conditions that might include consent; kept under secure conditions; and accessible to the individual for amendment or challenge.

The GDPR goes further into the realm of ethics, emphasising principles that were not previously so prominent. These include transparency (or openness) and accountability, both of which address the ethical and practical relationship between controllers and processors of personal data and individuals, and reflect the OECD Principles. In another direction, the GDPR appears to go beyond the question of protecting individual's rights by drawing attention to the general *societal* interest in the protection of individuals" rights, for example in Article 57(1)(b), which says that a supervisory authority must "promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing". This codifies an existing practice in which supervisory authorities have for many years been engaged as societal "educators" in raising public awareness as part of their portfolio of tasks[18], although this role was not specified in the Directive.

16 Revised in 2013. See The OECD Privacy Framework http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf).

17 Council of Europe (1980), *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention 108). This was modernised in 2018 as Convention 108+, CM/Inf(2018)15-final. Note that Convention 108+ also embraces "dignity": its Explanatory Report states that: "Human dignity requires that safeguards be put in place when processing personal data, in order for individuals not to be treated as mere objects" (para 10.).

18 BENNETT, C. and RAAB, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd edn. Cambridge, MA: The MIT Press, p. 139-40. Article 15 of Convention 108+ includes awareness-raising among the duties of supervisory authorities.

There are practical reasons for raising the level of public understanding about information processing and rights, but there is also an ethical dimension: awareness-raising could contribute to the shaping of societal conditions and an "ecosystem" for privacy and data protection that would be considered socially beneficial in the information age.

3 THE INCREASING PROMINENCE OF ETHICAL DISCOURSE

Beyond the GDPR and data protection more generally, in recent years there has been a proliferation of more directly ethical discourse in the data protection community among commercial and governmental data controllers, as well as supervisory authorities, featuring the formation of ethical codes of practice, ethics advisory processes and groups, and an increasing awareness of data ethics.[19] Alongside the EDPS initiative mentioned earlier, other examples include a report of the UK Information Commissioner's Office on big data, artificial intelligence, machine learning and data protection, with an emphasis on ethical approaches in data protection[20]. Further than this, and in the private sector, the Information Accountability Foundation[21] now includes ethics in its work among business and other data controllers[22]. However, it is often unclear what this ethical "turn" amounts to, how it relates to legal requirements, and what practices it enjoins on (or forbids to) whom; moreover, what its proponents mean by "ethics" is often not explained. Sceptics and critics of the efficacy of ethical and "responsible" approaches to information systems, data-driven innovations such as AI, and the like point to their powerlessness and the merely formulaic and pious terms in which ethical precepts are typically framed. These criticisms are often well argued, and the way in which data--related activities and regulatory or self-regulatory proposals by business or government are disguised by cosmetic ethical wrappers is easily shown. Nevertheless, doing what one should do with personal data, and refraining from what one should not do, are increasingly on the agenda and are likely to feature prominently in the implementation of the GDPR. Part of this agenda includes efforts for creating an effective ethical culture in which

19 See RAAB (2020), *supra* note 7, and the sources cited therein.

20 Information Commissioner"s Office (2017), *Big data, artificial intelligence, machine learning and data protection*, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

21 Information Accountability Foundation (IAF) (2017), *Artificial Intelligence, Ethics and Enhanced Data Stewardship*.

22 RAAB (2017), *supra* note 9.

all stakeholders "do the right thing'[23], not as a substitute for enforceable legislation but as a complement to it.

Thinking ethically about the processing of personal data often causes dilemmas because judgment may be involved in situations where the line between "should" and "should not" is not clear. Moreover, ethics-based decision-making in "wicked" situations often points up the question of who is morally responsible for the "wrong" decision: a question that is not identical to the question of who is legally liable for it. Data controllers" declarations of the importance of ethical conduct in the "information age" may be a first step. There are also signs of genuine ferment and re-assessment as practitioners seek to understand the extra-legal implications of what they are doing, and to seek guidance towards decisions that involve something more than compliance with the law.

The search for ethical frameworks might denote the emergence of an information– (and information technology –) driven society in which risks and harms to human rights and social relations are taken more seriously. This development could also contest the prevailing approach in which convenience, commercial gain, and mission-oriented public policies take precedence in various contexts where personal data are processed. Of course, compliance with enforceable legal obligations should be most important; the strength of the GDPR lies in the fact that it contains clear rules and that breaches of the law are subject to sanctions, such as – but not only – considerable administrative fines..However, compliance needs reinforcement by ethical and rights-based precepts, if only to avoid a minimalist approach to data protection. Compliance with legal obligations should neither be driven by the prevailing approach mentioned above, nor by an attitude in which compliance would involve a mere check-list. Adopting ethical ways of data processing should be part of the DNA of organisations.

The role of ethics could become reinforced if the general public perceives that something is "not right', rather than 'not legal", in evaluating the data-driven processes to which they are increasingly involved. Recent controversies about the activities of Facebook, Instagram and other social media, as well as about Cambridge Analytica, serve to indicate that, more vocally than before, customers and citizens may press for ethically better

23 HIJMANS, H. (2018), "How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?", *European Data Protection Law Review* 1, with reference to the work of Christopher Hodges.

treatment rather than acquiescing in how they are dealt with by data controllers. However, perceiving and acting on the importance of ethical criteria is difficult in the contemporary global "datafied" society with its ubiquitous availability of personal information, especially when the means and purposes of data processing are not sufficiently clear[24]. In an information society in which power has shifted towards those who collect, share and hold large quantities of personal data[25], the GDPR might contribute significantly to giving these and other ethical principles some purchase to reduce the imbalance of power.

4 SURVEILLANCE: ITS ETHICAL IMPACT ON HUMANS

Surveillance is a key feature of a datafied society, and is facilitated or enabled by ubiquitous and often incomprehensible technology that is proving very difficult to regulate. There are many forms of surveillance or monitoring of individuals and groups: watching, listening, locating, detecting, and data monitoring[26] ('dataveillance", or the processing of personal data by business, governmental and social actors). Surveillance becomes even more intrusive when these forms are combined. The development of new technologies has expanded the possibilities and forms of surveillance, their interrelationships, and the ways in which they are used in a variety of contexts. These practices are driven by various economic, political, and social motivations that may be ethically dubious, and have a further negative effect on social values or rights, including privacy. The evolution of technologies brings forth increasing opportunities for surveillance that data protection laws and other safeguarding systems, including the GDPR, are designed to mitigate or sanction. However, new means of surveillance – coupled with, for example, automated decision-making on the basis of the data that is gathered – make many conventional safeguards obsolescent and irrelevant, stimulating further proposals for regulating AI.

24 MAYER-SCHÖNBERGER, V. and CUKIER, K. (2013) *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, [place of publication]: Eamon Dolan/Houghton Mifflin Harcourt.

25 HIJMANS, H. (2016) *The European Union as Guardian of Internet Privacy*, Law, Governance and Technology Series 31, at 3.6.

26 This section is adapted from RAAB, C. and WRIGHT, D. (2012) "Surveillance: Extending the Limits of Privacy Impact Assessment", p. 363-383 in Wright, D. and De Hert, P. (eds.), *Privacy Impact Assessment*. Dordrecht: Springer. For more detailed discussion, see Ball, K., Lyon D., Murakami Wood, D., Norris, C. and Raab, C. (2006) *A Report on the Surveillance Society*, for the Information Commissioner by the Surveillance Studies Network (SSN). http://ico.crl.uk.com/files/Surveillance%20society%20full%20report%20final.pdf; http://www.ico.gov.uk/news/current_topics.aspx; Monahan, T. (ed.) (2006). *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York, NY: Routledge.

Surveillance and its regulation therefore require a closer look through the lenses of fresh and sometimes fundamental questions. Gary T. Marx calls for an ethics for the "new surveillance'[27]; he contends that ethical concerns – beyond procedural rules – have not tended to be raised about information collection or surveillance activities. He identifies three broad areas of importance: the means by which the data are collected; the contexts in which these processes take place; and the uses, purposes or goals for which the data are collected, or by which people are tracked, monitored, watched, overheard, or detected. Within these areas, Marx poses a number of ethical questions to be asked about surveillance systems. Some of the provocative – and political – questions he asks concern equality: "Is the means widely available or restricted to only the most wealthy, powerful, or technologically sophisticated?"; "Within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist?"; and "If there are means of resisting the provision of personal information are these means equally available, or restricted to the most privileged?". Another question relates to the essence of human dignity and harm to the individual: "Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational, or spatial border)?" Situational norms may be violated in ways that are not only unpleasant or uncomfortable, but that may harm individuals" interests, including their ability to either engage in certain social or political relationships or to withdraw from contacts by choice, as well as the exercise of their rights. In the wider context of machine learning, data and analytics may lead to beneficial or "pleasant" outcomes whilst also causing harm to the interests and rights of individuals.

Three causes of concern about surveillance are important in the debate on the ethical and legal dimensions of the GDPR:

a. *Legality*: the GDPR constitutes a system of rules and principles defining the legality of data processing. However, since these rules and principles cover a wide range of situations, they are by definition formulated in an open and general manner. Hence, the GDPR does not always provide certainty whether a particular surveillance practice is legal or not. For example, it does not specify the obligations of operators if surveillance is covert, as may be the case in some law-enforcement deployments, or if

27 MARX, G.T. (1998) "An Ethics for the New Surveillance", *The Information Society*, 14(3), p 171-86. See also Raab (2012), *supra* note 9.

surveillance takes place in a non-transparent manner, as may happen in commercial or public-service contexts. Moreover, surveillance in the public sector is to a large extent left to the discretion of national jurisdictions, under Article 23. Finally, a surveillance practice may be legally and ethically challenged because it is not compatible with the data protection principles of Article 5, such as fairness and transparency.

b. *Power implications*: surveillance implies a power relationship between the surveillant and the surveilled, in which the surveilled's power disadvantage may result in personal harm. This imbalance of power and its potential harmful consequences have important ethical dimensions. The GDPR requires in specific situations that these imbalances be taken into account, for instance in the balancing that is required when personal data are processed in the legitimate interest of the controller (Article 6(1)(f)), or in the application of the provisions on profiling and automated decision-making.[28]

c. *Differential effects of surveillance*: surveillance may adversely affect some individuals, groups, or categories of persons more than others. This may depend on how targets of surveillance are chosen (e.g., mass, or targeted on individuals or groups), or on how the placement of surveillance technologies inadvertently captures data from some people and not others because of the non-random way in which different persons, or kinds of person, may be exposed to the particular devices in question. Deliberate targeting, failure to anticipate differentials, mass data collection and analysis for public policies and purposes, and the maldistribution of privacy and other human rights caused by surveillance can all be questioned on ethical grounds, beyond what the law may or may not say.

Modern surveillance poses the question whether the GDPR and other legislative instruments can effectively keep surveillance within bounds that preserve human rights and liberties, or whether we need a renewed emphasis on the ethical principles that should underpin these legislative instruments, an emphasis that should also be inculcated in the training and

28 Notably, Article 22.

practice of technology innovators and the companies or governments in which they work. The results of such enquiry can inform the application of the GDPR or, in the longer term, a debate on the need for innovations in the GDPR, in other legislative instruments, or in non-legislative instruments such as codes of conduct, certification, or guidance by the European Data Protection Board (EDPB), national supervisory authorities (DPAs), and other official and unofficial bodies. The regulative effect of an elevated public awareness may also be enhanced by orienting it towards ethical and human--rights dimensions that have greater public resonance than do the legislated rules that are derived from them.

5 ETHICS AS PART OF DATA PROTECTION LAW

Section 2 above introduced the close relationship between data protection – and, more specifically the GDPR – and ethics. The fundamental right to data protection gives an individual a claim that her data is being processed in a fair manner[29]. Other obvious value notions within data protection are human dignity and personal autonomy[30]. In addition, ethical considerations play a role in the application of data protection law, including the GDPR. In a rapidly changing information society in which threats from the "new surveillance" are increasingly palpable, the application of the GDPR has to be based to a considerable extent on understandings of the way in which dignity, fairness and other values are implicated in the management processes whereby the law is put into practice in actual contexts, and on judgements about the compatibility of these situations with the realisation of, for example, a liberal democratic society based on the rule of law and human rights.

Ethical analysis is becoming part of the application of data protection law, situating the ethical content of data protection principles and the human-rights rationale of data protection law "on the ground". Some of the GDPR's Recitals imply ethical principles – for example, regarding discrimination and social disadvantage, in Recitals 71, 75 and 85 – and provide a handle for further analysis. Implementing the GDPR requires judgement; data protection law cannot – and should not – be merely technically applied. According to the Court of Justice of the EU (CJEU), this is even a key reason

29 Article 8(2) Charter. See also the three basis criteria of Article 5(1) GDPR: lawfulness, fairness and transparency.

30 See HIJMANS (2016), *supra* note 22: 2.8.2.

behind the independence of DPAs[31]. These authorities are required to "balance" individuals" rights with the economic interest of the free flow of data. Balancing, or reconciling, various interests is also at the core of the processing of personal data for the purposes of the legitimate interest pursued by the controller or a third party, in accordance with Article 6(1)(f). More generally, processing for "legitimate interest" purposes becomes increasingly important, requiring contextual assessments[32], including a balancing between fundamental rights and market dimensions. Balancing – however it is done, and despite the ambiguity of the term – should heed the ethical precept that data protection is a human right; its essence, and that of other rights and ethical values, should always be respected[33], especially where the "balance" is between a fundamental right and an economic or other interest, policy, or convenience[34].

We do not claim that the balancing of different interests always requires deep ethical judgements. However, balancing acquires an ethical dimension when it includes the weighing of moral values or human rights and, hence, a judgement about what is good and bad for an individual and society. This is specifically the case when the vague norms of the GDPR must be applied in situations of rapid change, in which the law itself does not give clear answers. Moreover, the GDPR itself contains a number of components that may require an ethical judgement, when applied. For example, Article 24, the general provision on the obligations of the controller, introduces a risk-based approach. It specifies that the controller must take into account "the risks of varying likelihood and severity for the rights and freedoms of natural persons". Recital 75 describes specific risks and harms to rights and freedoms of individuals that deserve protection. Its application may involve

31 CJEU, Case C-518/07, Commission v. Germany: 30.

32 NISSENBAUM, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.

33 Article 52(1) Charter.

34 For critical views of "balancing" where human rights and freedoms are involved, see Raab, C. (1999) "From Balancing to Steering: New Directions for Data Protection", p. 68-93 in Bennett, C. and Grant, R. (eds.), *Visions of Privacy: Policy Approaches for the Digital Age*, Toronto: University of Toronto Press; RAAB, C. (2017) "Security, Privacy and Oversight", p. 77-102 in Neal, A. (ed.), *Security in a Small Nation: Scotland, Democracy, Politics*. Cambridge: Open Book Publishers, https://www.openbookpublishers.com/resources/9781783742684/Security-Small-Nation-ch3.pdf; Chandler, J. (2009) "Privacy Versus National Security: Clarifying the Trade-Off", p. 121-138 in Kerr, I., STEEVES, V. and LUCOCK, C. (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Oxford: Oxford University Press; more generally, DWORKIN, R. (1977) *Taking Rights Seriously*, London: Duckworth; WALDRON, J. (2003) "Security and Liberty: The Image of Balance", *Journal of Political Philosophy*, 11(2): 191-210.

balancing these risks of data use with the benefits of data use in a developing information society, but this judgement is not straightforward.

In any balancing exercise, the beneficial contribution that privacy protection itself makes to society, and not only to the individual "data subject", has to be taken into account[35]. Understanding privacy protection's practical benefit to society is not always sufficiently appreciated in data protection law. For example, it could be argued that the quality of public services and official statistics is compromised if people have little confidence that their data would be adequately protected against breaches or unauthorised disclosure, and therefore give false information about themselves to doctors or public agencies. Similarly, the data subject's right to rectification under Article 16, underpinned by the "accuracy" requirement in Article 5(1)(d), illustrates the important contribution that the exercise of data subjects" rights – enshrined in data protection law – may make to the quality of data, whether held for commercial or public-service purposes: no-one would argue that defective databases are part of the common good. In addition, the contribution that privacy and human-rights protection make to the development of a "data-driven" economy and society by enhancing the public's trust and confidence in AI, data analytics and the use of algorithms is frequently proclaimed in programme rhetoric, although how far it is taken seriously is yet to be determined.

An ethical judgement to be made is whether one can require an individual to contribute to a "greater good" in another sense: more specifically, to hand over his or her personal data for increasing the quality of public services, for which the use of personal data using big data analytics may significantly benefit society by increasing the accuracy of services. This question frequently arises in the domain of health and medicine, with specific reference to the use of patient data in research. Examples can be found not only in health (how to prevent and cure cancer), but also in education (how to combat school drop-out) and in transport (how to meet the needs of passengers in public transport).[36] Ethically-loaded issues surrounding consent, the re-purposing of data, scientific research, and the transparency

35 See REGAN, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, NC: The University of North Carolina Press, chapter 8; Raab, C. (2012), "Privacy, Social Values and the Public Interest", p. 129-151 in Busch, A. and Hofmann, J. (eds.) "Politik und die Regulierung von Information" ["Politics and the Regulation of Information"], *Politische Vierteljahresschrift* Sonderheft 46, Baden-Baden: Nomos Verlagsgesellschaft.

36 Examples from Information Commissioner"s Office (2017), *supra* note 19: 27.

of data-sharing are implicated in the pressures towards using personal data for "social benefit" or "public good". At the same time, individuals are entitled to control over their personal data and should be in a position to have a say, at least, in the disposition of their personal data. The claim of individuals is even stronger where there is a risk to their rights and freedoms, such as privacy, as explained in Recital 75 and as recognised in Article 9 on the processing of special categories of data, such as medical data.

6 ACCOUNTABILITY AND CORPORATE SOCIAL RESPONSIBILITY IN THE GDPR

Ethical behaviour is an integral element of accountability and of corporate social responsibility. A key concept is the principle of accountability as laid down in Article 24[37]. This requires data controllers to implement the necessary measures to ensure compliance and to be able to demonstrate that they have taken these measures. Both components are part of the legal responsibility of the controller, whereas the second component includes a procedural requirement to report, thereby demonstrating or giving an account of what they have done[38]. It is important to underline that accountability goes beyond legal responsibility. Legal responsibility concerns who is supposed to do what; it may involve legal implications for the performance or non-performance of roles and tasks, and for compliance with rules, as indicated in the GDPR. It may also involve authority relationships within organisational hierarchies, and demonstrating compliance to the supervisory authority and to the public at large[39], as far as this is explicitly required by the GDPR. Accountability, however, also implies that a responsible agent endeavours to respect the underlying principles of privacy and data protection and demonstrates its compliance or role-fulfilment even when this is not explicitly required by the GDPR.

Both the narrower legal responsibility and the wider principle of accountability involve ethical behaviour in two senses: in *performing*

37 Article 24 says "responsibility" instead of "accountability". The term "accountability" only appears in Article 5(2) and Recital 85. "Responsibility" is mainly used because there is no equivalent for "accountability" in a number of other languages (in particular, French). In the French language version, the term "responsabilité" is used for both responsibility and accountability. See the discussion of these two concepts in Raab, C. (2012) "The Meaning of "Accountability" in the Information Privacy Context", p. 15-32 and De Hert, P. (2012) "Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law", p. 193-232, both in Guagnin, D., HEMPEL, L., ILTEN, C., KROENER, I., NEYLAND, D. and POSTIGO, H. (eds.) *Managing Privacy through Accountability*, London: Palgrave Macmillan.

38 RAAB (2017), *supra* note 9.

39 For instance, by the annual report of the supervisory authority, as laid down in Article 59 GDPR.

according to the GDPR (insofar as its provisions are underpinned by ethical precepts), and – through giving an account of what one has done – in *explaining* this performance to others (i.e., the public or its representatives): in this way exemplifying one meaning of the principle of transparency. Accountability includes a risk-based approach[40] that may encourage data controllers to make ethical judgements, as they might do in undertaking a data protection impact assessment (DPIA): thus data controllers are required to evaluate risks to individuals" rights. Fairness is also recognised as an element of accountability, as in Article 5(1), where "fairly" is listed along with "lawfully and "in a transparent manner" with reference to the processing of personal data[41].

Moreover, accountability (including risk assessment) goes beyond compliance with the law. It is closely linked to corporate social responsibility, which makes companies responsible for their impact on society, integrating societal concerns into their business practices[42]. A parallel can be drawn with corporate social responsibility in the field of the environment. Others have developed the notion of enhanced accountability, also including ethical dimensions.[43]

There is also a link to responsible innovation (or responsible research and innovation). Where, as it is often claimed, the law cannot keep up with new technology, it may be a task for business to ensure responsible innovation.[44] To be responsible, innovation should be coupled with justified concerns for privacy, taking into account future uses of technologies and their possible privacy implications as well as consequences for other human rights[45]. Ethical organisations wish to do "the right thing'[46], and these good

40 As explained in earlier sections.

41 Centre for Information Policy Leadership (2015) "The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society", https://www.informationpolicycentre.com/cipl-white-papers.html; Raab (2017), *supra* note 9.

42 HIJMANS, H. (2016) *The European Union as Guardian of Internet Privacy*, Law, Governance and Technology Series 31: 6.14. See the remarks of the UK Information Commissioner, Elizabeth Denham, in her speech, "GDPR and Accountability", 17 January 2017, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/

43 Centre for Information Policy Leadership (2015), *supra* note 40.

44 JONES, M. (2017) "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw", https://ssrn.com/abstract=2981855.

45 Stahl, B. (2013) "Responsible research and innovation: The role of privacy in an emerging framework", *Science and Public Policy* 40: 708-716.

46 An essential element of ethical business practice; see Hodges, C. (2017 "Ethical Business Practice & Regulation: A Revolution in Regulation, Delivery, Enforcement and Compliance", *The 2017 Max Watson Lecture*, http://www.fljs.org.

intentions may give an ethical underpinning of activities relating to the processing of personal data. To quote Kant: "Nothing in the world – indeed nothing even beyond the world – can possibly be conceived which could be called good without qualification except a *good will*"[47]. Ethical behaviour also has a deontological dimension. The good will of organisations, as expressed in serious efforts, is part of accountability (or corporate social responsibility) under the GDPR. These principles are elaborated in various obligations for data controllers such as data protection by design and DPIA. It is safe to say that these specific instruments have an ethical dimension and should be applied to stimulate ethical behavior, not mainly as instruments for legal compliance. It is also possible, as some have shown, to go beyond a DPIA to develop an ethical or a social impact assessment, looking beyond privacy to the effects of surveillance on a wider range of human rights and values, both individual and collective[48].

An issue not yet discussed is whether this wide scope of accountability and responsibility – including ethical choices – implies that legal responsibility for compliance would also include moral responsibility for taking ethical considerations into account. This is an issue without an obvious solution. On the one hand, it is difficult to imagine that a large fine would be imposed by a DPA on a company for not taking ethical considerations into account beyond what is explicitly required by the GDPR. On the other hand, ethical choices may be the subject matter of a civil procedure on compensation and liability (as foreseen in Article 82) and could be included in judicial assessments in these cases.

7 HUMAN INTERVENTION AS A SPECIFIC ETHICAL COMPONENT OF THE GDPR

The ethical value of fairness is directly implicated in Article 22, which provides that individuals "shall have the right not to be subject to a decision based solely on automated processing", save for exceptions. The same Article provides that – where an exception to the main rule applies – an

47 KANT, I. (1959 [1785]) *Foundations of the Metaphysics of Morals*, trans. Beck, L. New York, NY: The Liberal Arts Press: 9, emphasis in original.

48 See, for example, WRIGHT, D. (2011) "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, 13(3): 199-226; Wright, D. and Friedewald, M. (2013) "Integrating privacy and ethical impact assessment", *Science and Public Policy*, 40(6): 755-766; Wright, D. and Raab, C. (2012) "Constructing a Surveillance Impact Assessment", *Computer Law & Security Review*, 28(6): 613-626; Raab and Wright [2012], *supra* note 25.

individual has nevertheless a claim to obtain human intervention[49]. Article 22 reflects the view that important decisions for individuals should be made by humans, not by mathematical models, in what is sometimes called the "age of algorithms'[50]. Automated decision-making may dehumanise individuals or social processes[51]. Individuals must have the right to exercise influence over decision-making processes that significantly affect them[52]; whether they have the (equal) ability to exercise this influence – and whose responsibility it should be to enable them – raises further ethical issues[53]. As will be seen later on, topical developments such as AI and, related to this, machine learning, engage ethical questions that are reflected in the EU's proposed AI Act.

Machine learning can be defined as "the set of techniques and tools that allow computers to 'think' by creating mathematical algorithms based on accumulated data"[54]. To simplify it, the more data computers can use, the better they learn, insofar as the training data is relevant and unbiased. An argument in favour of automated decision-making is that it is supposed to be fairer or more efficient[55] or effective. A machine is said to be fairer because it eliminates human bias when decisions are made, for example, about whether to allow a person to enter a foreign country. It can also be more efficient: a well-trained algorithm will decrease the risks of false

49 In the post-Brexit UK, a government consultation paper (DCMS 2021) asked whether Article 22 should be removed from UK GDPR legislation, as had been proposed by the Prime Ministerially-appointed Taskforce on Innovation, Growth and Regulatory Reform (2021). The Information Commissioner"s Office (2021) expressed concern with this proposal, as it would weaken the protection of individuals, and proposed instead the extension of Article 22 to cover human review of partly automated systems.

50 This is a key narrative in O"Neil, C. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, NY: Crown Publishing Group/Penguin Random House.

51 Bygrave calls this dehumanisation of social processes. Bygrave, L. (2014), *Data Privacy Law, An International Perspective*, Oxford: Oxford University Press. See also Jones, M. (2017), "The right to a human in the loop: Political constructions of computer automation and personhood", *Social Studies of Science* 47(2): 216 –239.

52 See on this provision, MENDOZA, I. and BYGRAVE, L. (2017) "The Right not to be Subject to Automated Decisions based on Profiling", *University of Oslo Faculty of Law Legal Studies Research Paper Series* No. 2017-20, at 3.

53 Some of the questions Marx asked about surveillance relate to automated decision-making: *e.g.*, "Is there human review of machine-generated results?" and "Are people aware of the findings and how they were created?" See: Marx (1998), *supra* note 24. These have a very contemporary ring some 20 years after, especially concerning debates about the "right to an explanation" in the GDPR, *e.g.*, Wachter, S, Mittelstadt, B. and Floridi, L, (2017) "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, 7(2: 76-99.

54 LANDAU, D. (2016) "Artificial Intelligence and Machine Learning: How Computers Learn", *iQ*, 17 August, https://iq.intel.com/artificial-intelligence-and-machine-learning/

55 Fairness and efficiency are main themes in Zarsky, T. (2016) "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness", p. 118-132 in *Automated and Opaque Decision Making, Science, Technology,* & *Human Values*, 41(1), without concluding that machines are fairer or more efficient.

positives or false negatives. However, more importantly, algorithms change our perspective because of the absence of human scale. Transparency is rendered very difficult: it is not feasible to explain choices of the algorithm to the individual, and there are also doubts to what extent it is feasible to inform an individual in a meaningful manner about the logic involved[56]. A dilemma here relates to the extent to which individuals are entitled or able to challenge machine learning and decisions based on it for reasons of data protection (e.g., the requirement of fairness) and other relevant laws concerning, for example, equality, even if the learning is thought to be beneficial for society. It is very difficult for an individual to challenge the results produced through a machine in case of a biased or defective algorithm or because the individual's specific case does not fit the category in which the algorithm has classified her. Where an algorithm produces an unfair or incorrect outcome – in other words, a false positive or false negative – the burden of proof for the individual may be extremely high.

In certain cases, a solution was found, providing individual redress. Two examples are given here. The first involves the right to be forgotten or the right to be delisted, the issue at stake in three cases before the EU Court of Justice involving Google[57]. Where an algorithm produces certain results in a search engine leading to the disclosure of publications relating to an individual, the individual needs to act to undo these results if they prove to be unfair; in these cases, the disclosure of irrelevant and harmful information relating to an individual on the Internet, The CJEU required individual redress with human intervention. The second example is the case of Bettina Wulff, the former wife of the former President of Germany. When people searched her name on Google Search, terms like "prostitute" and "escort" appeared, because the information was published based on algorithms. She had to act to undo the negative effects, bringing a lawsuit against Google to have these results undone[58]. We also discover an ethical issue resulting from automated processing: should a provider of Internet services take (proactive) measures to avoid harm to individuals" privacy? A possible ethical answer could be

56 As required by Art 15(1)(h). See: Centre for Information Policy Leadership (2017), "Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR", 19 May, at 2.8, http://www.informationpolicycentre.com.

57 CJEU, Cases C-131/12, C-136/17 and C-507/17.

58 As explained in Jones (2017), *supra* note 50.

that we cannot rely on AI by itself; human involvement should remain in the lead, and the notion of "meaningful human control'[59] should prevail.

8 ETHICS IN THE EU'S PROPOSED AI ACT

Section 7 above touched on automatic decision-making, machine learning, algorithms and the ethical principles that are relevant to contemporary AI innovations. In all domains – *e.g.* health, education, law enforcement, transport, "smart" living, commerce, communications, finance, and many more – the advent of AI poses a strong challenge to the norms, values, laws and other regulatory instruments that were framed in terms of "data protection", "privacy" and personal data". In a society that is not only "datafied" but "data-driven", the adequacy of this conceptualisation and, more specifically, of the regulatory and governance ecosystem that evolved in terms of these frames come under question. The GDPR to a large extent renewed and strengthened the application of legal rules and the ethical precepts that relate to them, giving them wider geographical reach and reforming regulatory machinery, roles and relationships. The EU's proposal for AI regulation carries this ethical basis forward and presupposes as well as complements the GDPR's implementation, but focuses specifically on AI as the subject for a legal regime that is similarly informed by ethical norms. How adequately it fulfils this remit is open to debate.

Its context is important to note in assessing its merits and shortcomings. The proposal was not created in a vacuum, free of ethical discourse. It was closely preceded by the post-GDPR work of the European Commission's High-Level Expert Group on Artificial Intelligence (ECHLEG), which produced ethics guidelines for trustworthy AI[60]. These guidelines have become widely known, even amidst the welter of similar materials produced by many organisations in the flourishing "turn" to ethics, and are referred to in the draft AI Act's Explanatory Memorandum (sec. 3.2). ECHLEG identifies four principles, called "ethical imperatives" and alternatively referred to as rights, principles and values: respect for human autonomy, prevention of harm, fairness, and explicability. These principles are grounded in fundamental

59 JONES, M. (2020) "The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles", *Vanderbilt Journal of Environment and Technology Law,* 18(1): 77-134.

60 European Commission High-Level Expert Group on Artificial Intelligence (2019) *Guidelines for Trustworthy AI*. For further discussion of this and other prominent sets of principles, see Raab (2020), *supra* note 7 and the sources cited therein.

rights, human-centricity, and concern for individual and societal benefit, and constitute an ethical top level of an elaborate architecture. This includes "requirements for trustworthy AI" under the headings of human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental wellbeing, and accountability. Further down the chain there are more specific items, including technical and non-technical methods of operationalising trustworthy AI that involve 23 themes and a checklist of 60 questions and 69 sub-questions for an envisaged pilot exercise in analysing AI systems to test their ethical compliance.

The proposal is risk-based, with different types of AI categorised in terms of the risks they are deemed to pose. The proposal's heaviest regulation is carefully limited in scope to situations in which there is a "high risk" to fundamental rights and safety from any particular use of AI by itself for as a component of products, taking into consideration its "intended purpose" and not apparently covering unintended consequences. AI systems or products considered not to be of high risk are dealt with by voluntary measures such as codes of conduct (Recital 81 and Article 69), and there is also a category of prohibited AI (Article 5) that includes covert manipulations aimed at distorting a person's behaviour (but subject to a harm test), and certain law-enforcement deployments of remote real-time biometric identification systems that can, however, be authorised for use.[61]

In the eyes of some critics, the draft law is "stitched together from 1980s product safety regulation, fundamental rights protection, surveillance and consumer protection law'[62]. The risk, therefore, is that the fundamental rights and ethical values enshrined in the proposal's worthy intention may be compromised by the way in which the regulatory regime has been conceived and crafted. A powerful engine driving the proposal is the encouragement of the further development and implementation of AI in all domains without stifling innovation with onerous restrictions. As the Explanatory Memorandum (sec. 1.1) puts it, "this proposal presents a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked

61 For more detailed comment on how the wording of Article 5 provides loopholes, see Veale, M. and Zuiderveen Borgesius, F., (2021) "Demystifying the Draft EU Artificial Intelligence Act", *Computer Law Review International*, 22 (4). See also the review of their article by Kaminski, M. (2021), "The Law of AI", *Technology Law JOTWELL*, October 25.

62 Veale and Zuiderveen Borgesius (2021), *supra* note 60: 26.

to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market".

Adherence to ethical principles and the protection of fundamental rights is, to be sure, incorporated into the proposal, but it may be the weaker commitment in face of the powerful business and state interests in developing and deploying AI, and the application of the AI law may require more relevant machinery that is closer to the domain of rights protection. The mechanisms of the GDPR, protecting the rights of the data subject, could have served as an example for the application of practical ethics to regulating the broad field of AI in which the acknowledged potential risks and harms to individuals and groups would be addressed by solid regulatory and legal measures of broad applicability. Clarke's analysis indicates grounds for scepticism about the salience of the ethical notions in the draft AI Act. He develops a framework of ethical and practical requirements with 10 overarching "themes" and 50 "principles" and uses it as a yardstick for evaluating laws and policies that purport to promote or regulate ethical and responsible AI. [63] Whereas the ECHLEG guidelines score 74 % in conformity to his framework, the draft AI Act achieves 50%, with great variation across the fourfold risk levels for AI systems and many absent principles. It gains very low scores on many specific principles and relatively few high marks[64]. He shows that, across the four risk-level categories in the proposal, there are many gaps, loopholes, exceptions and other contributory factors that lead to an overall judgement that the proposed legislation is a failure in terms of principles and ethics[65].

It is worth noting that the EDPB and the European Data Protection Supervisor (EDPS) issued a Joint Opinion on the proposed AI Act, in which – while welcoming the proposal generally – they emphasise further

63 CLARKE, R. (2019) "Principles and Business Processes for Responsible AI", *Computer Law and Security Review*, 35(4): 410-422. The themes are: assess positive and negative impacts and implications; complement humans; ensure human control; ensure human safety and wellbeing; ensure consistency with human values and human rights; deliver transparency and auditability; embed quality assurance; exhibit robustness and resilience; ensure accountability for obligations; and enforce, and accept enforcement of liabilities and sanctions. The principles are mainly more granular specifications under each theme, combining mundane procedural steps (*e.g.*, conduct audits of safeguards and controls) with lofty ethical precepts (*e.g.*, respect for individual autonomy, freedom of choice, and right to self-determination).

64 Clarke, R. (2021) "The EC"s Proposal for Regulation of AI: Evaluation against a Consolidated Set of 50 Principles" Review Draft of 22 August 2021, http://www.rogerclarke.com/EC/AIP-EC21.html.

65 CLARKE (2021), *supra* note 63: 10.

apprehensions and call for the strengthening of safeguards[66]. The views of the EDPS are in particular weighty because the draft Act empowers it as the supervisory authority for the activities of the EU's institutions, agencies and bodies (Article 59(8) and as the market surveillance authority (Article 63(6)) for the same. The EDPB and EDPS are concerned particularly with data protection in the strict sense, including the relationship between an AI Act and the GDPR and the existing institutional data protection regime, but with wider AI implications as well. They write (para. 2): "Generating content, making predictions or taking a decision in an automated way, as AI systems do, by means of machine learning techniques or logic and probabilistic inference rules, is not the same as humans carrying out those activities, by means of creative or theoretical reasoning, bearing full responsibility for the consequences." Moreover, AI "will erode our capability to give a causal interpretation to outcomes, in such a way that the notions of transparency, human control, accountability and liability over results will be severely challenged" (para. 3).

With regard to ethics, and specifically discrimination, the Opinion supports bans on social scoring, the use of AI for the automated identification of individuals" biometric or behavioural features in publicly accessible spaces, and the use of AI to sort people into clusters based on personal characteristics. Article 21 of the Charter of Fundamental Rights of the European Union[67] is invoked to underpin non-discrimination, and other international rights-based documents are also cited more generally where the impact of AI on society and individual gives rise to apprehensions. The Opinion criticises the proposal's deficiency in addressing individuals" rights and remedies (para. 18), but they also go beyond the question of individuals" rights in pointing to wider societal and political risks: for example, "Post remote biometric identification in the context of a political protest is likely to have a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy" (para. 31). Concerning the important value of transparency, the Opinion supports – with suggested further strengthening – the proposal for establishing a public register of

66 EDPB-EDPS (2021), *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*, 18 June, at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021--proposal_en.

67 EDPB-EDPS (2021), *supra* note 65, Executive Summary and para. 5, and paras. 27-35.

stand-alone high-risk AI systems (paras. 69-72), although Clarke sees this instrument of transparency as more seriously deficient[68]. The Opinion also criticises the Article 52 exemption from transparency requirements of certain AI systems that are used in criminal law-enforcement, on grounds of sustaining the presumption of innocence as well as rights and freedoms through safeguards, checks and balances that are important in a "well-functioning democracy" (paras. 70-72).

Clarke looks closely at the ways in which the proposal's provisions fall short of implementing ethical and principled-based considerations[69], while Veale and Zuiderveen Borgesius also illustrate the draft's shortcomings in practice, given the wording of clauses that restrict the application of prohibitions or rules: for example, with regard to the conditions under which AI-related manipulation of persons may be outlawed, and with regard to the use of biometric identification systems[70]. Clarke further observes that the legislative proposal for AI does not even reflect the EU's own ECHLEG guidelines: "Key expressions… such as "Fairness", "Prevention of Harm", "Human Autonomy", "Human agency", "Explicability", "Explanation", "Well-Being" and "Auditability", are nowhere to be seen in the body of the Proposal'[71]. These are unfortunate deficiencies, but we may observe an even greater discrepancy between what is said in the document's own preliminary Explanatory Memorandum and Recitals, and what is laid down in the Articles of the proposed law itself. While "fairness" appears nowhere, "transparency", "trust", "trustworthiness" and many other ethical and rights--related values do frequently occur in the proposal's preliminary sections, but are not included in the Articles. The preliminaries are rhetorically impressive in their coverage of ethical principles and in their well-intentioned emphasis on safeguarding fundamental human rights concerning, for example, non-discrimination and privacy, which, it is acknowledged, may be harmed by AI applications in which surveillance and bias are prominent[72].. The devil is in the detail of the Articles, and the detail hides behind the ethical window--dressing. We emphasise that the enforcement of the AI Act will mainly take place on the basis of what is included in Articles, not on the basis of the intentions of the legislators.

68 CLARKE (2021), *supra* note 63: Appendix 1A.
69 CLARKE (2021), *supra* note 63: Appendices 1A and 1B.
70 Veale and Zuiderveen Borgesius (2021), *supra* note 60: 4-5, 7-9.
71 CLARKE (2021), *supra* note 63: 10.
72 See, for example, Recitals 33, 35-40.

9 IN CONCLUSION: WHO SHOULD TAKE THE LEAD IN MAKING ETHICAL JUDGEMENTS?

Making ethical judgements would require specifying criteria for judging "good", "bad", 'right", wrong", and other ethical evaluative categories, beyond the question of legal compliance. These are moral judgements in areas where there is not necessarily consensus in a society or across societies. These types of judgement also go beyond the scope of data protection. Nevertheless, ethical judgements are increasingly becoming an integral part of the application of the GDPR, as they are in many other contemporary pieces of legislation and policy developments in the fields of information technology and systems, AI, and "data science" more generally. As we have seen, these judgements are part of the accountability of data controllers wanting to do the right thing. Also, DPAs, when performing their wide range of duties under Article 57, should be guided by ethical considerations, which should also play a role in the sanctioning regime. To give an example, Article 83(2)(b) provides that the imposition of administrative fines shall, *e.g.*, be based on the intentional or negligent character of an infringement. This relates to the good will and ethical judgement of the controller.

The GDPR should be applied in a legitimate, effective and consistent manner[73]. Hence, ethical judgements should be made on the basis of ethical standards, but those that are comprised by the GDPR are not sufficiently specific, and the draft of the AI Act falls short of its promise. The dual objective of EU data protection (fundamental rights protection, but also free movement of data)[74] does not help either, and may simply point up the tensions between conflicting ethical principles, as well as their ambiguous meaning. This applies as well to the regulation of AI, in which there is considerable tension between the economic and political interests in technological innovation and exploitation in the one hand, and ethical values and human rights on the other. If ethical standards should, hence, be formulated and at least refine the general notions of the GDPR, the question is who should take the lead in this process.

The starting point could be that data protection is an area where expert bodies (the DPAs as supervisory authorities for data protection) with complete independence from the executive and other branches of government – and

73 HIJMANS, H. (2016) *The European Union as Guardian of Internet Privacy*, Law, Governance and Technology Series 31, 2016, *e.g.* at 10.3. The consistency mechanism is included in Chapter VII, Section 2 GDPR.

74 As explained by Lynskey, O. (2015) *The Foundations of EU Data Protection Law*, Oxford: Oxford University Press.

free from any external influence – play an important role in the application of the law. They are responsible for enforcement and also for giving guidance to stakeholders. Surveillance is an example where the protection of individuals should not depend on the political preferences of the day or – indeed – on majoritarian public opinion about the primacy of safety or public order[75]. This argument is even stronger in relation to ethical issues, and makes it sensible to consider organising standard-setting mechanisms located a certain distance from government. However, this does not mean that the DPAs are in an obvious position to fulfil this role. The EDPS took an important initiative by setting up a short-life Ethics Advisory Group[76], as noted earlier. This early step may be a recognition that – possibly – a supervisory authority for data protection is not fully equipped by itself to set standards for making ethical judgements. This article is not the place to develop a model for the governance of ethics within the context of the GDPR, nor indeed in other contexts that concern specific – but widely ramified – technologies and systems, such as AI. However, a few observations can be made.

First, although organisations themselves should play a significant part in making ethical judgements as part of their accountability[77] – a process that could not be replaced by the mechanical application of precisely formulated ethical standards – the development of more widely applicable ethical standards may prove to be useful, to promote legitimacy, effectiveness and consistency. As this is a domain where wide consensus on "good" and "bad" is needed, it would therefore be important to ensure that industry and civil society can play a role. As far as business may be in the lead, it should engage with other stakeholders (e.g., civil society, governments), as many private-sector organisations are now doing.

Second, ethics committees at regional (such as the EU), national or sectoral level could play a role in developing or even adopting ethical standards and in guiding ethical judgements in specific cases[78]. Since

75 For further reading, see HIJMANS, H. (2016) *The European Union as Guardian of Internet Privacy*, Law, Governance and Technology Series 31, Chapter 7.

76 See *supra* note 8.

77 The perspective of how organisations might address the application of ethical data processing to new technologies is at the core of the Information Accountability Foundation's paper by Abrams, M., Abrams, J., Cullen, P. and Goldstein, L. (2019), "Artificial Intelligence, Ethics and Enhanced Data Stewardship", *IEEE Security & Privacy*, 17(2).

78 An example is the European Group on Ethics in Science and New Technologies (set up by the European Commission) (2018), *Statement on Artificial Intelligence, Robotics and "Autonomous" Systems,* 9 March, https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1.

consistent approaches are needed in an information society with constant cross-border data flows, it is important that the big ethical questions should not be reserved for the national or even regional level. Where possible, consistency on ethical issues should not be limited to the EU itself and perceptions on ethics in other parts of the world should be included in the thinking process, but the possibility of worldwide, cross-cultural agreement on ethics and on the desirable extent to which they should prevail is likely to be remote.

Third, this should neither replace nor diminish the role of DPAs, which could develop views on how to include ethical considerations in the application of data protection laws, such as – within the European Union – the GDPR. An ethics committee (or multiple ethics committees) advising the DPAs could play a role here.

REFERENCES

ABRAMS, M.; ABRAMS, J.; CULLEN, P.; GOLDSTEIN, L. (2019). Artificial intelligence, ethics and enhanced data stewardship. *IEEE Security & Privacy*, 17(2).

BENNETT, C.; RAAB, C. (2006). *The governance of privacy: policy instruments in global perspective*. 2nd edn. Cambridge, MA: The MIT Press.

BLACK, J. Forms and paradoxes of principles based regulation. *LSE Legal Studies Working Paper*, No. 13, 2008.

BYGRAVE, L. *Data privacy law, an international perspective*. Oxford: Oxford University Press, 2014.

CHANDLER, J. Privacy versus national security: clarifying the trade-off. *In*: KERR, I.; STEEVES, V.; LUCOCK, C. (eds.). *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Oxford: Oxford University Press, 2009.

CLARKE, R. Principles and business processes for responsible AI. *Computer Law and Security Review*, 2019.

CLARKE, R. *The EC's proposal for regulation of AI: evaluation against a consolidated set of 50 principles*. Review Draft of 22 August 2021. Disponível em: http://www.rogerclarke.com/EC/AIP-EC21.html.

CLIFFORD, D.; AUSLOOS, J. Data protection and the role of fairness. *Yearbook of European Law*, 2018.

DE HERT, P. *Accountability and system responsibility*: new concepts in Data Protection Law and Human Rights Law, 2012.

DWORKIN, R. *Taking rights seriously*. London: Duckworth, 1977.

EDPB-EDPS. *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*, 18 June. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021--proposal_en.

FLORIDI, L. *The ethics of information*. Oxford: Oxford University Press, 2013.

GUAGNIN, D.; HEMPEL, L.; ILTEN, C.; KROENER, I.; NEYLAND, D.; POSTIGO, H. (eds.). *Managing privacy through accountability*. London: Palgrave Macmillan.

HIJMANS, H. *The European Union as guardian of internet privacy*: Law, Governance and Technology Series 31, 2016.

HIJMANS, H. *The European Union as guardian of internet privacy*. Law, Governance and Technology Series 31: 6.14. See the remarks of the UK Information Commissioner, Elizabeth Denham, in her speech, "GDPR and Accountability", 17 January 2017. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/.

HIJMANS, H. *The European Union as guardian of internet privacy*. Law, Governance and Technology Series 31, 2016, *e.g.* at 10.3. The consistency mechanism is included in Chapter VII, Section 2 GDPR.

HIJMANS, H. *The European Union as guardian of internet privacy*. Law, Governance and Technology Series 31, Chapter 7, 2016.

HIJMANS, H. How to enforce the GDPR in a strategic, consistent and ethical manner? *European Data Protection Law Review 1*, 2018.

HODGES, C. *Ethical business practice & regulation*: a revolution in regulation, delivery, enforcement and compliance, 2017.

JONES, M. *Does technology drive law?* The dilemma of technological exceptionalism in cyberlaw. 2017. Disponível em: https://ssrn.com/abstract=2981855.

JONES, M. The right to a human in the loop: political constructions of computer automation and personhood. *Social Studies of Science*, 2017.

JONES, M. The ironies of automation law: tying policy knots with fair automation practices principles. *Vanderbilt Journal of Environment and Technology Law*, 2020.

KAMINSKI, M. The law of AI. *Technology Law JOTWELL*, October 25, 2021.

KANT, I. (1785). *Foundations of the metaphysics of morals*. Trans. Beck, L. New York, NY: The Liberal Arts Press, 1959.

LANDAU, D. Artificial intelligence and machine learning: how computers learn. *iQ*, 17 August. 2016. Disponível em: https://iq.intel.com/artificial-intelligence-and-machine-learning/.

LYNSKEY, O. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

MARX, G. T. An ethics for the new surveillance. *The Information Society*, 14(3), 1998.

MAYER-SCHÖNBERGER, V.; CUKIER, K. *Big data: a revolution that will transform how we live, work, and think*. [place of publication]: Eamon Dolan/Houghton Mifflin Harcourt, 2013.

MENDOZA, I.; BYGRAVE, L. The right not to be subject to automated decisions based on profiling. *University of Oslo Faculty of Law Legal Studies Research Paper Series,* No. 2017-20, at 3, 2017.

NISSENBAUM, H. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press, 2010.

O'NEIL, C. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York, NY: Crown Publishing Group/Penguin Random House, 2016.

RAAB, C. From Balancing to steering: new directions for data protection. *In*: BENNETT, C.; GRANT, R. (eds.). *Visions of Privacy: Policy Approaches for the Digital Age*. Toronto: University of Toronto Press, 1999.

RAAB, C. Privacy, social values and the public interest. *In*: BUSCH, A.; HOFMANN, J. (eds.). Politik und die Regulierung von Information ["Politics and the Regulation of Information"], *Politische Vierteljahresschrift Sonderheft* 46, Baden-Baden: Nomos Verlagsgesellschaft, 2012.

RAAB, C. Regulating surveillance: the importance of principles. *In*: BALL, K.; HAGGERTY, K.; LYON, D. (eds.). *Routledge Handbook of Surveillance Studies*, London: Routledge, 2012.

RAAB, C. *The meaning of "accountability" in the information privacy context*, 2012.

RAAB, C. Information privacy: ethics and accountability. *In*: BRAND, C.; HEESEN, J.; KRÖBER, B.; MÜLLER, U.; POTTHAST, T. (eds.). *Ethik in den Kulturen – Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn*. Tübingen: Narr Francke Attempto, 2017.

RAAB, C. Security, privacy and oversight. *In*: NEAL, A. (ed.). *Security in a Small Nation: Scotland, Democracy, Politics*. Cambridge: Open Book Publishers, 2017. Disponível em: https://www.openbookpublishers.com/resources/9781783742684/Security-Small-Nation-ch3.pdf.

RAAB, C. Information privacy, impact assessment, and the place of ethics. *Computer Law and Security Review*, 37, July, 2020. Disponível em: https://authors.elsevier.com/sd/article/S0267-3649(20)30009-1.

RAAB, C.; WRIGHT, D. Surveillance: extending the limits of privacy impact assessment. *In*: WRIGHT, D.; DE HERT, P. (eds.). *Privacy Impact Assessment*. Dordrecht: Springer, 2012.

REGAN, P. *Legislating privacy: technology, social values, and public policy*. Chapel Hill, NC: The University of North Carolina Press, 1995.

STAHL, B. Responsible research and innovation: the role of privacy in an emerging framework. *Science and Public Policy*, 2013.

VEALE, M.; ZUIDERVEEN BORGESIUS, F. Demystifying the draft EU artificial intelligence act. *Computer Law Review International*, 22 (4), 2021.

WALDRON, J. Security and liberty: the image of balance. *Journal of Political Philosophy*, 2003.

WRIGHT, D. A framework for the ethical impact assessment of information technology. *Ethics and Information Technology*, 2011.

WRIGHT, D.; FRIEDEWALD, M. Integrating privacy and ethical impact assessment. *Science and Public Policy*, 2013.

WRIGHT, D.; RAAB, C. Constructing a surveillance impact assessment. *Computer Law & Security Review*, 2012.

ZARSKY, T. The trouble with algorithmic decisions: an analytic road map to examine efficiency and fairness. *In*: *Automated and Opaque Decision Making, Science, Technology, & Human Values*, 41(1), 2016, without concluding that machines are fairer or more efficient.

Sobre os autores:

Hielke Hijmans | *E-mail:* hielke.hijmans@gmail.com

President of the Litigation Chamber of the Belgian Data Protection Authority, Professor International and European Data Protection Law at the Vrije Universiteit Brussels.

Charles Raab | *E-mail:* c.d.raab@ed.ac.uk

Professorial Fellow, Politics and International Relations, School of Social and Political Science, University of Edinburgh.

Artigo convidado.