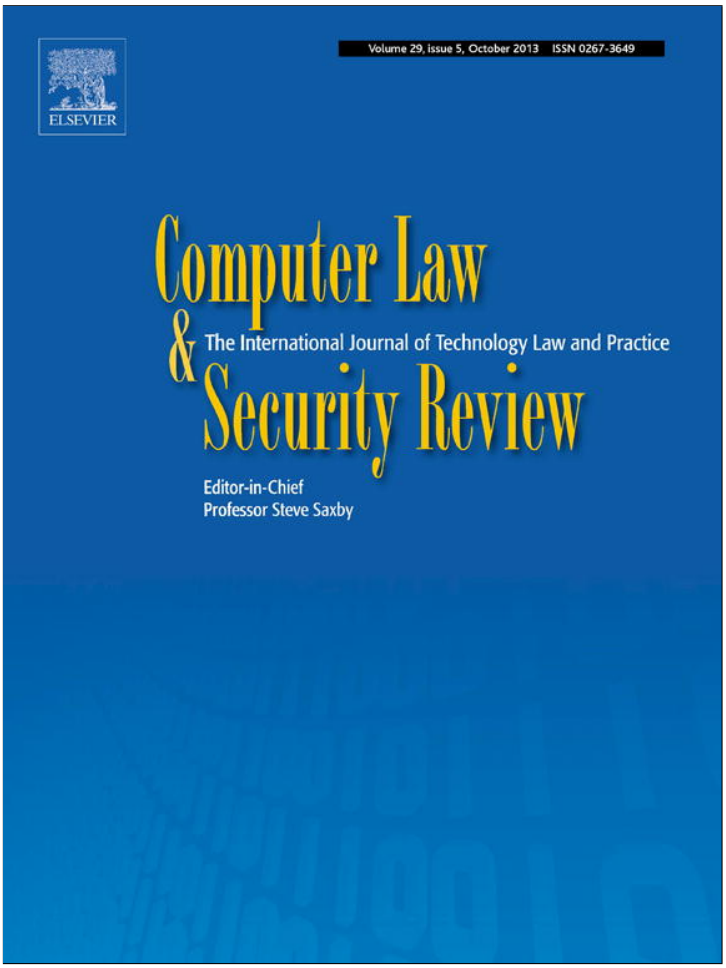
2013

# Data Protection by Design and Technology Neutral Law

Mireille Hildebrandt, *Radboud University Nijmegen*
Laura Tielemans, *Vrije Universiteit Brussel*



COMPUTER LAW & SECURITY REVIEW 29 (2013) 509–521

Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

# Data protection by design and technology neutral law

*Mireille Hildebrandt* [a], *Laura Tielemans* [b]

[a] *Radboud University, Nijmegen, Netherlands*
[b] *Vrije Universiteit Brussel, Brussels, Belgium*

*Keywords:*
Technology neutral law
Data protection by design
Personal data processing systems
Compensation
Innovation
Sustainability
Legal certainty
Fundamental rights
Non-discrimination

ABSTRACT

This article argues that to achieve a technology neutral law, technology specific law is sometimes required. To explain this we discriminate between three objectives, often implied in the literature on technological neutrality of law. The first we call the compensation objective, which refers to the need to have technology specific law in place whenever specific technological designs threated the substance of human rights. The second we call the innovation objective, referring to the need to prevent legal rules from privileging or discriminating specific technological designs in ways that would stifle innovation. The third we call the sustainability objective, which refers to the need to enact legislation at the right level of abstraction, to prevent the law from becoming out of date all too soon. The argument that technology neutral law requires compensation in the form of technology specific law is built on a relational conception of technology, and we explain that though technology in itself is neither good nor bad, it is never neutral. We illustrate the relevance of the three objectives with a discussion of the EU cookie Directive of 2009. Finally we explain the salience of the legal obligation of Data Protection by Design in the proposed General Data Protection Regulation and test this against the compensation, innovation and sustainability objectives.



## 1. Three objectives of technology neutral law

This paper will research the technological neutrality of the European Union (EU) legislative framework, with special attention for data protection by design (DPbD). Because our focus is on EU legislation, the terminology of technological neutrality will be determined in view of the aim of the EU legislator to enact and sustain effective legal norms. Though we target digital information and communication technologies (ICTs) and personal data processing systems (PDPSs) we note that any type of legislation is in fact technologically specific, since our environment is always technologically mediated. For instance, our interactions are mediated e.g. by the printing press, drugs, sewage systems, railway infrastructure or housing projects. We have specific legislation on the freedom of the press, copyright, public transport, water supply or municipal architecture. Insofar as the legislation addresses our default technological environment this usually goes unnoticed,[1] and only when rapid technological change requires specific legislative responses do lawyers and politicians speak of a need for technology specific law.

In this section we sketch three interpretations of technology neutral legislation: first we discuss the idea that in order to be neutral, the law may have to provide for technology specific

[1] This is connected with the question of how law itself is technologically mediated. This mediation differs between oral societies, and those of the script, the printing press and the emerging digital information and communication infrastructure is another game changer. On the difference between 'technology neutral law' and 'technologically neutral law' see section 3 below.

0267-3649/$ – see front matter 
http://dx.doi.org/10.1016/j.clsr.2013.07.004

provisions to retain the substance of the legal right they support. This is usually framed as ensuring equivalent effect in online and offline environments. Second, we discuss the idea that legislation should not discriminate between different types of technologies with the same functionality or between mainstream and emerging technologies, because this could stifle innovation and result in unfair competition. Third, we discuss the need for legislation to be reasonably future proof in the sense that legislative acts take a long time to be constructed and focussing on a specific technology may render the legislation outdated and ineffective sooner than expected.

According to the Bonn Ministerial Conference Declaration of 1997, whereby the Ministers of the European Member States (MSs) had the mission to agree on key principles to handle and regulate the fast developing Global Information Networks, 'the general legal frameworks should be applied online as they are offline. In view of the speed at which new technologies are developing, we will strive to frame regulations which are technologically neutral, whilst bearing in mind the need to avoid unnecessary regulation'.[2] The 1997 Ministerial Declaration states that technology should not be used as a shield to avoid the implementation of the fundamental rights of privacy and data protection. Whether a user is acting offline or online should not have an impact on the level of protection. Contrary to what one might conclude prima facie, this does not mean that the rules should be exactly the same, precisely because the legislator should provide for an equivalent protection online and offline.[3] Often, online technologies require a different legal approach to create similar effects of legal protection offline. The collapse of distance, the ease of publication and reproduction, hyper-connectivity, and affordances like automated remote control, high-speed interaction and invisible tracking and tracing are game changers for business models but also for effective legal protection. So, achieving the aim of particular fundamental rights by enacting different rules for online environments actually enables neutrality. This approach has e.g. been affirmed by the United Kingdom e-Principles: 'the effect of the offline and online regulatory environments should be as similar as possible'. In the same vein, the authors stress that 'there may be occasions when different treatment is necessary to realise an equivalent result'.[4] This correlates with the fact that in law equal cases must be treated equally, whereas cases that are not equal must be treated differently to the extent that the difference is relevant. The decision on what counts as equal cases is a normative, not merely a descriptive decision. For instance, all citizens, no matter how much they differ in race, sex, age, religion, ethnicity, or social background, need to obey the same criminal law that is applicable in their jurisdiction. With regard to these different citizens, the criminal law is neutral. It does not develop a specific criminal law for persons of different race or religion. The reason is that we believe this would be unjust. However, if we find that certain differences impact the effectiveness of legal norms, the law may apply some form of compensation to enhance e.g. the bargaining power or the socio-economic position of a person with a specific ethnic or religious background. In the case of gender, for instance, positive discrimination may be allowed or imposed. Similarly, in the case of consumers, their bargaining power in relation to large companies may be improved by means of legally enforceable consumer protection. The bottom line here is that whereas legal certainty and justice demand legislation that does not unduly discriminate,[5] in specific instances this demands legislative intervention to achieve a measure of substantive equality. The same applies to the treatment of different technologies: neutrality is default but to achieve this technology specific legislation may be required. One option to realize this, to be investigated in this chapter, is the use of technology itself to create equivalent protection, namely by means of DPbD, which confirms the need for 'technological specificity' as a means to achieve technology neutral legislation. We will refer to this objective as the compensation objective, which entails that under certain conditions technology specific legislation is required to compensate a detrimental impact of specific designs or usage of a technology on the effectiveness of legal norms.

In the 1999 Communications Review,[6] technological neutrality is seen in terms of 'rules [that] should neither impose, nor discriminate in favour of the use of a particular type of technology to achieve those objects.' Here we see that the objective of technology neutral legislation is to prevent an unfair competitive advantage for existing technologies or for specific companies that produce or employ one or the other technology. Similarly, the US Government Framework for Global Electronic Commerce states that 'rules should neither require nor assume a particular technology'.[7] In other words, as long as the rules do not single out and discriminate certain technologies, they can be considered neutral. The reason is that unjustified discrimination could result in interference with the market dynamics of competing technologies and create competitive disadvantages for other technologies. There is a strong link with interoperability and with novel notions such as data portability: for a fair and open market ineffective thresholds should be removed in order to allow all

[2] Recommendation 22, Bonn Ministerial Conference 1997, available at http://ec.europa.eu/archives/ISPO/bonn/Min_declaration/i_finalen.html.

[3] B.J. Koops, 'Should ICT Regulation be Technology-Neutral', in *Starting Points for ICT Regulation: deconstructing prevalent policy one-liners*, eds. B.J. Koops bewerkt door B.J. Koops, Miriam Lips, Corien Prins, en Maurice Schellekens (The Hague: TMC Asser, 2006), 77–108. Koops discusses this under the heading of 'What holds off-line should also hold on-line' (Koops 7-8). Chris Reed, 'Taking Sides on Technology Neutrality', *SCRIPT-ed* 4, nr. 3 (2007): 263–284. Reed discusses explicitly that 'technologically neutral rules addressing the same issue may well differ in their wording and content, in order to achieve the same (or at least broadly equivalent) *effects* when applied to these technologies' (Reed at 267, italics in the original).

[4] Koops, 'Should ICT Regulation be Technology-Neutral'. 2, the document on the UK principles he refers to is available at: <http://webarchive.nationalarchives.gov.uk/20040722012351/e-government.cabinetoffice.gov.uk/assetRoot/04/00/60/79/04006079.pdf>.

[5] Ibid. 5.

[6] European Commission, Towards a new framework for Electronic Communications Infrastructure and Associated Services. The 1999 Communications Review, COM (1999) 539, 10 November 1999, p. 25.

[7] US Framework for Global Electronic Commerce. (Title II, 3), available at: http://clinton4.nara.gov/WH/New/Commerce/read.html.

stake holders to create added value. This, however, does not imply that technologies that violate data protection by default cannot be discriminated against, in comparison with the same type of technologies with a more privacy friendly default. We will refer to this objective as the innovation objective, which entails that legislation should refrain from imposing unnecessary restraints on the development and employment of new technologies and business models.

The third interpretation of technology neutral legislation concerns the sustainability of particular legislative acts. To avoid the cumbersome procedure of reiterant law amendments, these acts for instance incorporate the competence to delegate specific regulation to be more flexible, or standard-setting to governmental bodies to be more specific, without going through renewed parliamentary debate. Another option is to include industry self-regulation or co-regulation based on guidelines that have no legal effect but should allow stakeholders to coordinate their behaviour in the market.[8] The objective of making legislation technology-proof is part and parcel of legal common sense: we condemn and criminalize murder, irrespective of whether it was committed with a knife, a gun or by pushing someone off a cliff. Spelling out the different instruments used to commit the offence has no added value and we will not write new laws every time a new instrument is developed that is capable of killing a person. However, this has not stopped legislators from enacting specific legal norms for telecom operators, the pharmaceutical industry or the sale of specific lethal weapons.[9] The point is not that legislation should always be technology-proof, but that technology specific legislation is only enacted if there is a necessity to address or to redress the impact of a technology on the substance of a legal right. We will refer to this objective as the sustainability objective, which entails that legislation should refrain from enacting detailed technology specific legislation that addresses societal problems caused by the affordances of a specific technology, if similar affordances can be expected for other existing or emerging technologies.

In section 3 we will see how DPbD relates to the three current understandings of technology neutral legislation. First, however, we will develop our own framework of testing legislation in terms of technology neutrality by investigating whether technologies themselves are neutral and how this affects the neutrality of the law. We use the example of cookie legislation to demonstrate the viability of the triple test of compensation, innovation and sustainability.

## 2. A framework for testing the technology neutrality of legislation

Generally speaking, legislation is not meant to be neutral. Legal acts are the outcome of a political debate between several stakeholders having different views of the general interest. The outcome of this political process will always entail the imposition of a specific legal normativity with specific legal effect. Hence, the rules that are constructed as a result of the legislative process have a normative bias. The term bias is not used in a pejorative way here, but as a reminder that law is meant to have a normative impact. In a constitutional democracy, the normative bias of legal rules combines the instrumental dimension of legal rules, which concerns their expedience to achieve certain objectives, with their protective dimension, which concerns the justice and the legal certainty they must provide. Legal certainty and justice share the aim of treating equal cases equally. Legal certainty also refers to the positivity of the law, which discriminates legal rules from moral or political rules. The instrumentality and the protective dimensions of the law embody its specific normative bias, which is intended as such. This implies that the neutrality of law in respect of different technologies requires that the law generates the same normative effect irrespective of the technological environment in which these norms apply.

Before developing our framework for testing the technological neutrality of specific legislation, we will engage with the question of the normative impact of technological environments, since this may interfere with the normative effects of the law. To this end we will briefly discuss different conceptions of the neutrality of technology itself.

### 2.1. *The neutrality of technology: instrumentalist, autonomous and relational conceptions of technology*

Autonomous or substantive approaches to technology claim that Technology, with a capital T, follows its own logic and has substantive and autonomous effects on social, economical, political, and historical developments. Within this view, society is understood as determined by technological developments. For instance, Jacques Ellul introduced the notion of the technological society as a new '*milieu*' between people and nature. What previously had only been determined by the laws of nature is now also thought to depend on 'laws' determined by technology. Ellul compares the self-determining, independent characteristics of nature with those of technology. Though technology is itself one of the ways to artificially employ the laws of nature, it generates a further dynamic that co-determines how people can shape their lives. Think, for instance, of cloud seeding or of cloning, or even the old fashioned dam constructed to stop the water current and generate energy.[10] By means of technology human beings change the nature, scope and impact of their environment, thus enlarging or limiting the range and cast of human interaction. Ellul goes one step further by stating that the human mind is dominated or even determined by technology, culminating in the point where the purpose of life and human happiness can only be achieved via Technology.[11] Applying this theory to the specific

[8] Koops, 'Should ICT Regulation be Technology-Neutral'. 11.

[9] Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach', *Harvard Law Review* 113, nr. 501 (1999): 501–547. Susan W. Brenner, *Law in an era of 'smart' technology* (New York: Oxford University Press, 2007).

[10] Take, for instance, the generation of energy: 'Energy is a primary resource for all activities, and by transforming energy generation, and the ability to distribute it to any location and to portable applications, humankind became able to increase its power over nature, taking charge of the conditions for its own existence,' M. Castells, 'Informationalism, Networks, and the Network Society: A Theoretical Blueprint.' In Manuel Castells, ed. *The Network Society: A Cross-Cultural Perspective* (Edward Elgar Pub, 2005), 8.

[11] Jacques Ellul, *The technological society* (New York: Knopf, 1964).

topic of data processing, we should take note of the complex setting in which these technologies are employed, as well as the complexity they generate. This makes it highly unlikely that all phenomena in our society can be reduced to pure inevitabilities of technological development. Surely, the power and economic growth associated with developing or using data mining software to figure out consumer behaviour and mapping patterns determines in a broad way strategic and commercial management decisions that lead to success and sustainability in the market. It is no secret that these technologies go one step further by making consumers believe they want to buy certain products, while they are unwittingly trading their data in exchange for the use of applications on e.g. smartphones or in social networking sites.

However, if one were to accept the autonomous theory for ICTs such as computing systems, mobile networking and wireless access, this would entail that we have little or no choice anyway, since the underlying logic of the technological infrastructure determines the general make-up of both the society and the individual person that depend on this infrastructure. Ellul may have a point here, because technological transformations such as the script, the printing press, the steam engine and electricity created novel environments from which neither people nor society could easily unplug. However, it should be clear that much depends on how these technologies are designed, how they are taken up, how they finally consolidate and to what uses they are put. Instead of focussing on the constraints generated by Technology in general, we prefer to focus on the many constraints and enablers brought into play by specific technologies and – especially – on the fact that different designs, different integration, different consolidation and differential use have entirely different effects. So, though they determine both individual and societal options, technologies leave much room to alternative design and integration, which leads us to conclude that technologies are underdeterminate. Also, the extent to which they determine depends on empirical characteristics of specific technologies used in a specific context, not on general attributes of Technology.

According to instrumentalist theories, technology is another word for tools or instruments created or used for a purpose. These purposes are determined by mankind; politics, the military, end users, businesses, they all use technology for certain reasons. It is these reasons that can render technology either good or bad. Technology *in se* is always neutral and can only be judged by its use.[12] Instrumentalist conceptions therefore clearly understand technology as neutral. The problem with instrumentalist theories is that they provide little understanding of the influence of a specific technology on issues of power and control.[13] In fact, a variety of technologies is embedded into daily activities that can be considered to have major impact on people's behaviour and social interactions, often restructuring their social dynamics. Andrew Feenberg rightly notes that if technology is considered to be neutral, then all the repercussions must be termed as merely accidental and unforeseen side effects.[14] Even if this were the case, however, accidental and unforeseen consequences invariably affect our environment and our capabilities. For this reason technology cannot be classified as neutral, regardless of the question of whether the effects were 'unforeseen'. This also relates to the common sense idea that '*guns don't kill people, people do*', which can be opposed to another common sense finding, namely Latour's idea that a man with a gun is a different man than a man without a gun.[15] For instance, the shift from the use of knives to that of guns as weapons changes the distance from which another person can be attacked; it enables killing someone without bodily contact. It changes the scope of assault and warfare. Similarly, the use of drones offers a whole new range of methods to kill people remotely, extending the distance at which killing is possible in a way that changes the scope and nature of targeted killing at the international level. Though it is clear that whoever uses his hands, a sword, a gun or drones to kill has responsibility for the choice to engage in such action, the availability of a certain type of instrument nevertheless changes the scope of the responsibility. Additionally, upcoming smart technologies that are automated and can function without human intervention again change the range of human interaction, the type and size of damage and suffering as well as the foreseeability of what has been called collateral damage. Authors such as Asimov and Chandler have described technology as something that might at some point be beyond human control, even developing a will of its own.[16] Instrumentalist theories do not provide the conceptual tools to explain how the law could deal with this. The loss of control that is inherent in techniques of artificial intelligence, such as neural networks and machine learning, demonstrate that high tech tools and smart machines do affect society and demand for regulation that evolves in response to technological development.[17]

Next to the substantive and the instrumentalist conceptions of the normative impact of technology, a third position has been developed, which highlights the instrumental,

[12] Peter F. Drucker, 'Technological trends in the twentieth century', in *Technology in Western Civilization*, vol. 2, 1967ste ed. (New York: New York University Press, z.d.).; Simon Ramo, *Century of mismatch*, 1St Edition (McKay, 1970).

[13] The canonical reference here is still: Langdon Winner, *Autonomous technology: technics-out-of-control as a theme in political thought* (Cambridge, Mass.: MIT Press, 1977). Also, Norman Balabanian, 'Presumed Neutrality of Technology', *Society* 17, nr. 3 (1 maart 1980): 7–14, where he refers to the theory of neutrality as an ideology.

[14] Andrew Feenberg, *Critical Theory of Technology* (Oxford University Press, USA, 1991).

[15] Bruno Latour, 'On Technical Mediation', *Common Knowledge* (3) 2 (1994): 29–64.

[16] Asimov, *Asimov on science fiction* (Doubleday, New York, 1981): 130; D. Chandler, *Technological or media determinism, Lecture notes* available at Aberystwyth University, see http://www.aber.ac.uk/media/Documents/tecdet/tecdet.html; Ellul, *The technological society*.

[17] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet of Things? An action plan for Europe (2009) COM (2009) 0278 final, see also the website for the 4th Annual Internet of Things Europe, 12–13 November 2012, available at: http://www.eu-ems.com/summary.asp?event_id=124&page_id=991, which explicitly addressed the issue of whether separate legislation is needed and whether the proposed Data Protection Regulation will be able to keep up with the Internet of Things.

enabling and constraining dimensions of technologies without falling prey to determinism or instrumentalism.[18] This third view can be coined as a pluralist or relational understanding of technological impact on human society. It highlights the plurality of normative impacts that a technological device or infrastructure generates, whether intended or unintended. It does not deny the instrumental dimension but does not succumb to instrumentalism; technologies are always more than a mere instrument because they change the options for human action. Moreover, by emphasizing the relational aspect of technological impact, this third position acknowledges that the consequences of technological interventions always depend on how individual human beings and societies engage with them. This way it becomes clear that alternative designs make a difference and must be explored if they affect the substance of e.g. human rights such as privacy.[19] To phrase it with Kranzberg: technology is neither good nor bad (as this would entail a substantive conception); but it is never neutral (as this would endorse an instrumentalist conception).[20]

### 2.2. *Technology neutral legislation for a specific technology: the Cookie Directive (2002/58/EC)*

To investigate how legislation can be technology neutral and to detect when it should be technology specific to ensure technology neutrality, we will discuss the so-called Cookie Directive. The ePrivacy Directive provides protection of data and privacy of users online.[21] In 2009 the Directive was amended by the Citizens' Rights Directive, often called the Cookie Directive,[22] because it added a requirement of prior and informed consent in the case that cookies are placed on a user's computer. The tracking of a users' device can lead to identifying the user of the device and is an intrusion of a user's privacy. In the context of the amended ePrivacy Directive prior and informed consent are required irrespective of whether the data collected is personal data, which broadens the scope of data protection as compared to that of the Data Protection Directive, which is only applicable if personal data are processed. The ePrivacy Directive only applies to public electronic communication networks, so it targets the use of a particular technology. In that sense it is not technology neutral. By imposing special legal rules for cookies, the ePrivacy Directive has engaged in an even more technology specific regulation. Already at the moment of its enactment a number of alternative technologies were available to trace and track consumers' websurf and clickstream behaviours across different websites. For instance, http authentication, browser fingerprinting, internet service provider (ISP) tracking via IP addresses and deep packet inspection (DPI) technology, speech recognition, and server logs analysis, where login data is being logged each time a user logs on to a site.[23] This demonstrates that overly specific regulation of a particular technology may miss its target precisely because of its specificity. In that sense it is an excellent example of the admonition not to develop legislation that requires recurrent updates, in this case every time a new technique for tracing and tracking consumers across the web is developed and used. A more effective and technology neutral articulation would have stipulated that prior and informed consent is required every time a user's online behaviour is tracked or traced without necessity.[24] Indeed, the art. 29 Working Party has interpreted the relevant provision in exactly that way, by stating upfront that 'As such, this opinion explains how the revised Article 5.3 impacts on the usage of cookies *but the term should not be regarded as excluding similar technologies*' (italics ours).[25] In fact, the wording of the provision in which the tracking technology is regulated (art. 5.3) does not mention 'cookies', but states that 'the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user has given his or her consent, having been provided with clear and comprehensive information (…), inter alia, about the purposes of the processing'. The industry has, not surprisingly, complained that the transition from the earlier opt-out rule (the right to refuse) to an opt-in rule is not feasible, because it is next to impossible to ensure compliance every time such technology is being used and because it would annoy the user who is confronted with banners requiring her reiterant attention and intention. Clearly, for current business models, this tracking data is valuable information, for instance to nourish the analytics that should improve the website experience (and its clout in terms of attracting profitable customers); enable behavioural advertising; and aid the fight against spam and malware. As behavioural economics has demonstrated, people tend to stick to the default settings of

[18] M. Hildebrandt, 'Legal and technological normativity: more (and less) than twin sisters', *Techné: Journal of the Society for Philosophy and Technology* 12, nr. 3 (2008): 169–183; Peter-Paul Verbeek, 'Materializing Morality. Design Ethics and Technological Mediation', *Science Technology & Human Values* 31, nr. 3 (2006): 361–380.

[19] M. Hildebrandt, 'Technology and the End of Law', in *Facing the Limits of the Law*, bewerkt door Erik Claes, Wouter Devroe, en Bert Keirsbilck (Dordrecht: Springer, 2009): 443–464.

[20] Melvin Kranzberg, 'Technology and History: 'Kranzberg's Laws'', *Technology and Culture* 27 (1986): 544–560.

[21] Directive 2002/58/EC.

[22] Directive 2009/136/EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws OJ L337/11 (18.12.2009).

[23] To the extent that such techniques manage to 'gain access to information already stored in the terminal equipment of a subscriber or user' they fall within the scope of art. 5.3, thus requiring prior informed consent. Recital 66 states that consent may be provided by means of browser settings.

[24] Though it seems focused on malware and spyware, Recital 65 refers to a broad category of tracking mechanisms, notably 'software that surreptitiously monitors the actions of the users', stating that 'a high and equal level of protection of the private sphere of users needs to be ensured'.

[25] Art. 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP194, 7 June 2012, at 2; cf. EU Commission Kroes in her Speech/2012/716 on online privacy and online business: An update on Do Not Track (DNT), where she states that DNT should apply to tracking technologies via cookies and also by other means. SPEECH/12/716, 11/10/2012, available at: http://europa.eu/rapid/press-release_SPEECH-12-716_en.htm#PR_metaPressRelease_bottom.

their environments (referring to the so-called status-quo 'bias').[26]

Companies are probably right in expecting that an opt-in obligation will cost them much of the behavioural data and thus also cost them part of their business. This has led many websites to develop a smart strategy: they ask visitors for consent to use cookies and explain that without cookies they will not be able to use the site or will have a dull user experience. They build on the inclination to follow default settings, using this 'bias' for their own advantage, by asking consent once and for all, claiming this will help consumers to get rid of recurrent requests for consent. Such a strategy, however, erodes the objective of the provision and misleadingly suggests that consent is required for all cookies. This is not the case. The provision articulates two exceptions from the informed consent requirement. The first exception concerns 'any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network' (art. 5.3). The art. 29 WP concludes that this concerns at least three types of cookies, namely those with '1) The ability to route the information over the network, notably by identifying the communication endpoints; 2) The ability to exchange data items in their intended order, notably by numbering data packets; 3) The ability to detect transmission errors or data loss'.[27] The second exception requires 'the storage and/or access of data to be strictly necessary for providing an information society service that has been explicitly requested by the subscriber or user' (art. 5.3).[28] The Art. 29 WP concludes that this applies when '1) A cookie is necessary to provide a specific functionality to the user (or subscriber): if cookies are disabled, the functionality will not be available; 2) This functionality has been explicitly requested by the user (or subscriber), as part of an information society service'.[29] In short, the storage or access of data must be essential to provide the requested service, such as a cookie that ensures that the information in the basket remains available when checking out to buy the selected products.[30] Interestingly, the Art. 29 WP continues with a detailed analysis of what types of cookies must be distinguished and how they fit with the consent requirement, and follow this up with similarly detailed discussions of the necessity requirement. It turns out that the difference between first and third party cookies depends, just like necessity does, on a number of factors that will differ between users, and will often depend on choices made or still to be made in other domains than the one at stake when deciding about acceptance of a particular cookie. Furthermore, next to session cookies, persistent cookies, first and third party cookies, we also have multipurpose cookies that make a requirement for granular consent difficult to implement. Finally, the Art. 29 WP discusses a number of 'cookie use case scenarios' that range from user-input cookies, to authentication cookies, user centric security cookies, multimedia player session cookies, load balancing session cookies, user interface customisation cookies, social plug-in content sharing cookies, and a series of non exempted cookies: social plug-in tracking cookies, third party advertising and first party analysis cookies. They then sum up seven guidelines on how to discriminate between cookies that do and those that do not require prior informed consent:

This analysis has shown that the following cookies can be exempted from informed consent *under certain conditions if they are not used for additional purposes* (our italics):

1) User input cookies (session-id), for the duration of a session or persistent cookies limited to a few hours in some cases.
2) Authentication cookies, used for authenticated services, for the duration of a session.
3) User centric security cookies, used to detect authentication abuses, for a limited persistent duration.
4) Multimedia content player session cookies, such as flash player cookies, for the duration of a session.
5) Load balancing session cookies, for the duration of session.
6) UI customization persistent cookies, for the duration of a session (or slightly more).
7) Third party social plug-in content sharing cookies, for logged in members of a social network.[31]

What does this example teach us about the possibility of technology neutral law in a case where a specific type of technologies has major impact on the effectiveness of legal precepts such as informational self-determination, purpose binding and necessity? If the goal is to ensure prior informed consent for tracing and tracking websurf behaviour whenever there is no necessity, then what does the example tell us about the need for technology specific legislation to ensure technology neutral legislation? Let us return to the discussion of technology neutral law above, which discriminated three objectives that can be summed up in terms of compensation, innovation and sustainability.

The first objective concerned the idea that the normative impact of e.g. human rights should not depend on whatever technologies are employed. If specific technologies interfere with the effectiveness of human rights, the legislator may have to address the design, manufacturing and usage of such technologies. The use of cookies to collect behavioural data in a way that is invisible and of which the consequences are difficult to foresee, interferes with human autonomy and may lead to prohibited or undesirable discrimination. If the legislator finds that compensatory legislation is necessary to rebalance the ensuing power and knowledge asymmetries, the most important condition for new legislation should be

[26] Richard H. Thaler en Cass R. Sunstein, *Nudge: improving decisions about health, wealth, and happiness* (New Haven: Yale University Press, 2008). Behavioural economics claims to have detected a set of irrational biases that inform human behaviour, rather than the previously assumed rationalist *homo economicus*.

[27] WP194, *Cookie Consent Exemption*, at 3.

[28] An 'information society service' refers to 'any service normally provided for remuneration, at a distance, by electronic means of electronic equipment for the processing and storage of data, and whereby at the individual request of a recipient of a service', cf. art. 1.2 Directive 98/34/EC. We will refer to these types of providers as 'service providers'.

[29] WP194, *Cookie Consent Exemption*, at 4.

[30] UK Information Commissioner's Office, Guidance on the rules on use of cookies and similar technologies, v.3. May 2012, 6, available at http://www.ico.gov.uk/news/blog/2012/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx and WP 194, *Cookie Consent Exemption*, at 5.

[31] WP194, *Cookie Consent Exemption*, at 11.

whether it indeed provides effective tools to reintroduce e.g. informational self-determination. The choice of the EU legislator has been to address this problem in the context of the ePrivacy Directive, which basically addresses telecom operators and is not applicable to information society services (all kinds of services providers other than those involved in mere data transmission). This would obviously restrict the application to a specific technical infrastructure, whereas most of the problems occur at the level of information society services. To achieve its objective the provision regarding cookies is, therefore, also applicable to information society services. On top of this (furthermore) the provision is not only applicable to personal data processing, but to any mechanism that captures online behavioural data of end-users, whether these data can be qualified as personal data or not. The requirement that should offer compensation is prior and informed consent. This regards a transparency obligation and an opt-in right. Both aim to rebalance the knowledge and power asymmetries resulting from the tracing and tracking of granular consumer behaviours, notably those that enable cross-contextual tracking, large scale data mining and refined personalisation. By forcing companies to explain that and how they are tracking behaviours consumers are given a better bargaining position in relation to the service providers.

It seems that the compensation objective indeed provides arguments to redress negative consequences on the effectiveness of current legal protection, to the extent that such redress is not already enabled in the more general Data Protection Directive (DPD). One can think of a number of arguments that the notion of prior informed consent for tracking and tracing is part and parcel of the DPD. The only problem would be that the DPD applies only to personal data processing, whereas the cookie provision in the ePrivacy Directive applies to any online behavioural data of end users captured by a specific type of mechanism. However, generally speaking, the ePrivacy Directive also applies only to the processing of personal data, so in this case an exception had to be made. Perhaps, by addressing the problem in another Directive that functions as a lex specialis with regard to the DPD, it became possible to circumvent an appeal of service providers to one specific ground that allows the processing of personal data, namely that of the legitimate business interest of a service provider. The logic of the DPD entails that if personal data processing can be based on such a business interest, it is allowed. Instead of entering complex discussions of what is legitimate in this area, the EU legislator simply address the technique of tracking and tracing, irrespective of whether personal data are involved, irrespective of the legitimate business interests at stake. This brings us to the second objective of technology neutral legislation.

The second objective of technology neutral law concerned the idea that legal regulation should not cause unfair competitive advantages for companies that employ, develop or produce e.g. existing, novel, or alternative technologies, because this could stifle innovation or create unfair constraints on free market behaviours. We can phrase this as the task of a legislator to ensure a level playing field where all stakeholders can engage in the creation of added value. This objective can be aligned with the ground for lawful personal data processing on the basis of a legitimate business interest. Since service providers will compete by designing for the best 'user experience' and use personalisation as well as other type of data mining to create a competitive advantage they seem to have a legitimate interest in the collection, storing and mining of the behavioural data of their potential customers. Addressing the power imbalances discussed under the heading of the compensation objective will have to be articulated in a way that retains or re-establishes a level playing field. It does not mean that merely because all stakeholders employ a business model that interferes with informational self-determination the legislator should refrain from obstructing this business model. If a democratic polity decides that the gains of such business models ('free' access to a number of information services and personalised services that provide for relevant information and pleasant user experiences) do not outweigh the loss (in terms of privacy and undesirable social sorting), than the task of the legislator is to articulate a threshold and develop a new plane for the level playing field. Thus, companies are invited to develop new business models that do not infringe privacy and non-discrimination, but this constraint will be imposed on all players in the market. The innovation objective thus requires that technology specific legislation does not create unjustified barriers to market entry or unjustified competitive advantages for developers or users of specific technologies. In the case of cookie legislation this would, for instance, entail that if different types of mechanisms are used for the same functionality of tracking and tracing, they should all be subject to the legal condition of prior informed consent. Not only those that are already on the market or only those that the legislator can currently foresee. This brings us to the sustainability objective.

The third objective of technology neutral law concerned the idea that legislation should not require continuous adaptation to emerging technologies. The reason is twofold: first, the procedure for legislative acts takes too much time to be effective on the short term, and second, legal certainty requires that the legal norms, which are meant to coordinate interaction, do not change at such speed that they can no longer provide for legitimate expectations as to how people, companies and technologies will behave. Both reasons are challenged in an era where emerging technologies continue to provide for game changers at an unprecedented speed. Regulators, businesses and end users are continuously confronted with the everyday consequences of high-speed transformations of what technology enables in terms of creating added value, new business models, but also in terms of fraud, malware attacks, child pornography, private and public surveillance and subliminal personalisation of search engines, advertising, pricing, insurance and law enforcement.

Smart legislation requires expecting the unexpected, vigilance in the face of recurrent "black swans",[32] preventing over- as well as under-inclusive provisions despite the fact that emerging technologies often change the scope of application of enacted legal norms.[33] The cookie legislation is a

[32] Nassim Taleb, *The black swan: the impact of the highly improbable*, (New York: Random House, 2007).

[33] A major problem occurs if a legislator does not understand the technology it targets, which may happen precisely because future usage of the same technology or alternative technologies with the same effect are not foreseen. See Reed, 'Taking Sides on Technology Neutrality', section 3.2.

case in point: due to the fact that many new mechanisms have been developed to track users, the current provision is under-inclusive – unless a teleological interpretation such as that of the Art. 29 WP is applied. At the same time we found that the industry is applying an over-inclusive interpretation to turn the tables on the default-bias: they require consent for technical and functional cookies that do not require consent and thus force consumer to a default of accepting tracking cookies. Rapid technological change is often said to be hampered by outdated legislation; it may be that the mere attempt to design technology neutral laws that 'hold' in the future is a lost cause that indeed erodes the moral and practical force of the law. Writing sustainable law thus ends up creating legal *uncertainty* its precepts are in fact unsustainable due to unforeseen impacts. Perhaps the only way to achieve sustainability in this domain is to combine a general requirement stipulating that at the level of the technical design data protection obligations must be met, if technically and economically feasible. This would incentivize technological innovation with regard to built-in data protection, because once such technology is state of the art it becomes the legal standard. In the next section we will investigate the proposed provision of Data Protection by Design in view of the compensation, the innovation and the sustainability objectives.

## 3. Data protection by design: an example of technology neutral law?

One of the most challenging aspects of the proposed General Data Protection Regulation (GDPR) is the obligation for data controllers to ensure Data Protection by Design. This seems to initiate a new type of legal concept, whereby law aligns itself with the earlier ethical and policy-oriented concept of Privacy by Design.[34] In the same proposal a concurrent legal obligation is introduced to ensure Security by Design. By enacting these types of duties as legal obligations the EU legislator inaugurates examples of what has been coined as legal protection by design (LPbD),[35] confronting us with a new articulation of legal norms: next to unwritten and written law, we now have something like digital law. Acknowledging that law has been articulated in unwritten principles, inferred from written codes, judgements and doctrinal treatises, should alert us to the fact that modern law is technologically dependent on speech, writing and the printing press. To make sense, law must align itself with the ICT infrastructure that prevails in a particular society. With the novel ICT infrastructure of interconnected computing systems we now witness the rise of a novel technological embodiment of legal norms. This will have substantial consequences for the force of law, because technical articulation of legal norms may be done in ways that ensure the self-execution of the norms.[36]

This has raised a number of questions about the difference between law and administration and the need to safeguard the right to disobey the law.[37] Using technology to implement or enforce legal norms has been coined as techno-regulation and the discourse on how this relates to current conceptions of law and regulation.[38] This highlights the fact that law itself is never 'technologically neutral', even if we may require that it is 'technology neutral'. The first relates to the articulation, embodiment or inscription of the law: oral law has different affordances than written codes, and these have different implications than a digital law that is 'written' into computer code. Whereas our use of the term 'technology neutral law' concerns the fact that legal effect *should not* depend on the particular technology that is used by the addressees of the law, we reserve the term 'technologically neutral law' for the misconception that the law *does not depend* on its articulation. Such a misconception entails a 'mentalistic' understanding of legal norms,[39] which – like a brain in a vat – do not depend on whether it regulates an oral society, a society that has developed the handwritten manuscript, or a society whose information and communication infrastructure depends on the printing press. We believe that this is an untenable position and refer to other work in which modern law's productive dependence on the printing press has been argued.[40] This means that law cannot be technologically neutral because it is always enabled by a particular technological ICT infrastructure. In this article we will not move into the issue of what it means for modern law to reinvent the force of law in its novel, digital articulation, but focus on whether such an alternative articulation still allows for 'technology neutral law'.

### 3.1. *The legal articulation of DPbD in the proposed GDPR*

The Art. 29 WP has argued that the principle of data protection by design should become a legal obligation to take technological data protection into account at the planning stage of PDPSs. This approach implies that technology is in fact open and capable of capturing values and norms other than those strictly related to technology protocols. The WP finds that the principle should be general and binding, and, as the need arises, regulations for specific technological contexts should

[34] Ann Cavoukian, *Privacy by Design …. Take the Challenge* (Ontario: Information and Privacy Commissioner of Ontario (Canada), at https://ozone.scholarsportal.info/bitstream/1873/14203/1/291359.pdf, 2009); Demetrius Klitou, 'Privacy by Design and Privacy-Invading Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century', *Legisprudence* 5, nr. 3 (2011): 297–329.

[35] Mireille Hildebrandt, 'Legal Protection by Design: Objections and Refutations', *Legisprudence* 5, nr. 2 (2011): 223–248.

[36] E.g. Danielle K. Citron, 'Technological Due Process', *Washington University Law Review* 85, 1249–1313.

[37] Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford: Oxford University Press, 2008).

[38] Ronald Leenes, 'Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology', *Legisprudence* 5, nr. 2 (2011): 143–169; Hildebrandt, 'Legal Protection by Design'.

[39] On the 'mentalistic' understandings of the human mind Hubert L. Dreyfus, *What Computers Can't Do: the Limits of Artificial Intelligence* (New York: Harper & Row, 1979).

[40] M. Ethan Katsh, *Law in a digital world* (New York Oxford: Oxford University Press, 1995); Ronald Collins en David Skover, 'Paratexts', *Stanford Law Review* 44 (1992): 509–552. Mireille Hildebrandt, 'A Vision of Ambient Law', in *Regulating Technologies*, bewerkt door Roger Brownsword en Karen Yeung (Oxford: Hart, 2008).

be adopted which require embedding data protection and privacy principles into such contexts.[41]

Art. 23.1 of the proposed GDPR formulates an obligation for data controllers to implement the relevant protection of personal data at the level of design:

> *Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*

By merely dissecting this provision we can conclude the following.[42] *First*, the obligation to implement DPbD addresses data controllers. This means that it targets users of the relevant data processing techniques and technologies, not their designers or manufacturers. The idea seems to be that by making data controllers responsible (and liable), they will force developers to come up with the right types of technologies. *Second*, the Regulation does not impose 'privacy by design'. Privacy and data protection are different, partly overlapping fundamental rights (cf. art. 7 and 8 of the Charter of Fundamental Rights of the European Union), and the legal protection by design that is imposed in art. 23 targets data protection obligations. This means that it only targets privacy insofar as implied in data protection.[43] This is a wise decision, also because privacy is an open and essentially contested concept,[44] and it would be very difficult to define which design actually protects privacy. This is connected with the fact that privacy is a liberty, which resists definition ex ante.[45] The fundamental right to data protection has been defined in terms of a set of relevant principles and policies, usually referred to as the Fair Information Principles (FIPs), and in the context of the GDPR it should be reasonably clear what requirements must be complied with, namely those stipulated in the Regulation.

Since the Regulation contains rules rather than principles and specified legal rights rather than liberties, it should be easier to translate the legal conditions that apply into technical requirements. The objective of DPbD is that 'the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'. It is interesting to note that the Regulation speaks of 'requirements', which may remind the reader of 'requirements engineering', one of the disciplines involved in privacy and security by design.[46] *Third*, the Regulation provides two conditions that inform the content of the obligation, namely technical and economic feasibility. This implies that data controllers will not be confronted with unreasonably costly requirements or with an obligation to integrate requirements for which no technical solution has yet been developed. At the same time, it forces them to implement technical solutions that are available if the cost is not prohibitive. Once technical solutions for particular legal obligations are on the market at a reasonable price, data controllers will have to use them or implement their own equivalent or better solutions. This should create the middle ground for developers of DPbD technologies, thus stimulating innovation in the market for technical DPbD solutions. *Fourth*, the Regulation determines that the obligation to implement DPbD is at stake, first, when developing data processing technologies and the business models they hope to enable or sustain, and second, when performing the actual processing of personal data – in other words, during business as usual. This should ensure that whatever seemed technically and/or economically infeasible during the design of the data processing system, will again be considered once the processing is in operation. This will require a dynamic attitude to DPbD, acknowledging that speedy innovation implies that data protection will be a moving target; if an organisation wants to gain from high speed transitions that have high speed impacts on data protection, they will have to follow up with high speed updates for their data protection mechanisms. *Fifth*, the provision speaks of 'appropriate technical and organisational measures and procedures', taking a broad view of 'design'. This is not merely about privacy enhancing technologies (PETs) but about the integration of technical and organisational measures into the business models of data controllers. What those technical and organizational measures are will be up to the controller to decide. To opt for the word 'appropriate' shows that the controller still has discretion concerning which technical measures or procedures he will implement. Furthermore, it is open for the controller to define what the purpose of the processing is, and whether it is necessary to process, collect, and store the data for that purpose.

One more point can be made if we look into paragraphs 3 and 4 of the provision:

> 23.3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in

[41] Article 29 Data Protection Working Party, 02356/09/EN, WP 168, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009, p. 3.

[42] In paragraph 2 of the provision the concept of Data Protection by Default (DPbDefault) is defined in terms of data minimisation (which requires consent or one of the other grounds for processing, combined with purpose specification and use limitation). This means that DPbDefault is a subset of DPbD under the Regulation. We will not discuss DPbDefault separately, as it is already implied in DPbD.

[43] P. De Hert en S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in *Privacy and the Criminal Law*, bewerkt door Erik Claes, Antony Duff, en S. Gutwirth (Antwerpen Oxford: Intersentia, 2006).

[44] W.B. Gallie, 'Essentially Contested Concepts', *Proc. Aristotelian Soc'ty* 56 (1956): 167–198.

[45] S. Gutwirth, *Privacy and the Information Age, Translated by Raf Casert* (Lanham Boulder New York Oxford: Rowman & Littlefield, 2002).

[46] Seda Gürses, Carmela Gonzalez Troncoso, and Claudia Diaz, 'Engineering Privacy by Design,' CPDP2011, available at https://lirias.kuleuven.be/handle/123456789/356730.

particular for data protection by design requirements applicable across sectors, products and services.
23.4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

This tells us that, *sixth*, the Commission may specify and concretize the requirements of DPbD by means of delegated acts, especially in the case of requirements that should apply across sectors, products and services. Such requirements may be phrased in terms of technical standards. These should allow the coordination of data protection designs across e.g. different companies, in different Member States. Whereas the general wording of the provision abstracts from specific technical solutions, paragraphs 3 and 4 enable technology specific interventions by the European Commission. The Commission can move faster than the European legislator and may thus be able to address the issue of sustainability of the DPbD obligation.

In the next section we will investigate how the six points articulated in art. 23 fare with the compensation, the innovation and the sustainability objectives of technology neutral legislation. Before performing this test we will briefly discuss the difference between regulation and law.

### 3.2. *Testing the compensation, innovation and sustainability objectives*

According to Koops, regulation 'does not regulate the behaviour of machines, except to the extent that machine behaviour influences people's behaviour'.[47] He defines regulation in terms of the social science conception of regulation as 'intended to achieve certain effects in society',[48] which implies that law is just one way to regulate human behaviour. Obviously his definition of regulation includes other – non-legal – forms of regulation, notably techno-regulation, for instance when legislators or other regulators use technologies 'to achieve certain effects in society'.[49] In fact, all kinds of manipulation fall within the ambit of the social science definition of regulation, notably the use of behavioural economics (which is basically a branch of cognitive psychology) to 'nudge' people into specific behaviours.[50] From the perspective of a constitutional democracy, law is both more and less than regulation. It is more, because law does not only consist of legislation but also of adjudication, which provides the means to contest the application of legal norms and connects the singularity of an individual case with the generality of the applicable rule. Some authors may even claim that adjudication is the heart of the law because it decides on the meaning of legal code. Law is also less because legislation is enacted by a democratic legislator, whereas regulation may be initiated by any other stakeholder. Moreover, law does not condone manipulation, because its effectiveness cannot be measured exhaustively in terms of behavioural targets.

Legal rules are not a matter of regularity but of normativity, they should 'work' as standards for interaction that create legitimate expectations.[51] If compliance is enforced by means of threats and rewards that treat people as pawns instead of agents, we are no longer in the domain of law but in that of discipline or administration. The discourse of regulation speaks the language of behaviours, attempting to find effective tools to make people behave one way or another. The discourse of law speaks the language of action, addressing people as agents that are ultimately the authors of the rules that govern their interactions. This is why law is not necessarily about the regulation of effects, but also about treating people as having a mind of their own, capable of giving reasons for their actions. Indeed, one could say that the obligation to implement DPbD is meant to guarantee the design of an ICT infrastructure that provides people with the *means* to develop their agency, acknowledging that this cannot be taken for granted. The rights and obligations of data protection legislation must then be understood as *enabling* a person to invent and reconstruct her identity, supplying the tools for a measure of self-determination with regard to the volunteered, observed and inferred data that give others a measure of power over the person concerned.

#### 3.2.1. *As to the compensation objective*

To the extent that current or future business models and their enabling technologies inadvertently or even deliberately deprive a person of the substance of the right to data protection, technology specific legal norms may be required to compensate the ensuing infringements of these rights, thus ensuring the technology neutrality of the law. The need for technology specific law is generated by the normative effects of personal data processing systems (PDPSs), notably their effects on privacy, non-discrimination and due process of law. These systems have thus been recognized as non-neutral technologies, generating the need for technology specific legislation to safeguard an equivalent level of protection. DPbD basically follows the technology specificity of current data protection legislation, but it adds a novel dimension to the legal obligation to comply. This dimension refers to the fact that whoever employs PDPS must anticipate how the design of these systems impacts compliance,[52] and proactively prevent infringements of the GDPR by designing the PDPS in a way that prevents violation. The first point of the

[47] Koops, 'Should ICT Regulation be Technology-Neutral', 6.
[48] Ibid. 6. The most often quoted definition of regulation is found in J. Black, 'Critical Reflections on Regulation', *Australian Journal of Legal Philosophy* 27 (2002).
[49] On the difference between law and regulation S Gutwirth, P. De Hert, en L. De Sutter, 'The trouble with technology regulation from a legal perspective. Why Lessig's optimal mix' will not work', in *Regulating Technologies*, bewerkt door Roger Brownsword en Karen Yeung (Oxford: Hart, 2008), 193–218.
[50] Thaler and Sunstein, *Nudge: improving decisions about health, wealth, and happiness*. One of the founding fathers of this particular approach to human behaviour is Daniel Kahneman, 'A perspective on judgment and choice: Mapping bounded rationality', *American Psychologist* 589 (2003): 697–720.
[51] J.F.G. Glastra van Loon, 'Rules and Commands', *Mind* LXVII, nr. 268 (1958): 1–9.
[52] This is visible in the obligation to perform a data protection impact assessment (DPIA) in art. 33 of the GDPR. See David Wright en Paul de Hert, *Privacy Impact Assessment* (Dordrecht: Springer Netherlands, 2012).

DPbD provision discussed above entails that the obligation to provide for effective compensation is attributed to the data controller. Some have argued that this obligation should also be attributed to developers of technologies,[53] even if they are not data controllers. If technologies have normative impacts and cannot be considered neutral, the compensation objective seems to require that the obligation applies across the board.

In fact, the fourth point made above highlights that the obligation to implement DPbD applies in the stage of deciding on the means of data processing, which concerns the decision to invest in specific technologies. If a company develops its own PDPS this means that it is obligated to develop its systems with DPbD. In that case the obligation applies to the developer of PDPSs, whereas in the case that a company invests in PDPSs built by others, no such obligation applies to the developer of the technology. This seems to discriminate between two types of technology developers and it is unclear whether the compensation objective justifies such discrimination. We will return to this point under the innovation objective. The second point entails that the compensation regards infringements of data protection, thus only targeting privacy insofar as it is protected by data protection rules and policies. At the same time the compensation also targets the infringement of other fundamental rights, notably that of discrimination, insofar as they are protected by data protection rights and policies. By requiring DPbD at the early stage of decision-making regarding technology investment and/or technology development, as well as the later stage of its employment DPbD ensures substantive protection against the erosion of legal protection. This also compensates for the fact that technology developers who are not data controllers are not addressed directly. The anticipation of data protection infringements and the obligation to act on this should compensate for the impact of PDPSs that turn the tables on individual self-determination. In as far as DPbD involves higher costs for companies or governments working with PDPSs this is justified by the need to address and redress the infringement of fundamental rights that would otherwise occur.

#### 3.2.2. *As to the innovation objective*

The obligation to implement DPbD is not technology specific in the sense of stipulating which particular PDPSs it addresses, or in the sense of explaining which particular technologies should be used to achieve DPbD. As such, it seems compatible with the innovation objective. No PDPSs are excluded from the applicability of the obligation; no technological solutions are imposed, so no unfair competitive advantage is provided either way. As indicated above, the obligation does discriminate between technology developers that are also data controllers and those that merely sell PDPSs to data controllers. Only the former are obligated to integrate DPbD. This may obstruct innovation, because software companies that sell PDPSs may decide not to anticipate potential data protection infringements, which could mean that the state of the art does not develop in the direction of DPbD. On the other hand, however, the normative impacts of technologies depend on the context of their employment. It may be hazardous to foresee the normative impact of a technology that is not yet operational and can be used for a variety of purposes, many of which may not entail any infringements of data protection legislation. Requiring technology developers to anticipate any potential usage that may cause infringement could also stifle innovation. By addressing data controllers the provision ensures that those who hope to benefit from the use of PDPSs (the data controllers) have to bear the cost of liability when infringing data protection legislation. This should incentivize data controllers to invest in compliant design. Whether they make this investment through their own research and development departments or by investing in compliant PDPSs developed by other players, should not really make a difference. If, however, empirical findings demonstrate a reluctance on the side of technology developers to design for data protection, something like product liability may help to level their playing field.

DPbD is technology specific in its requirement that all data controllers must design or redesign the operations of their PDPSs such that they fit with the Regulation. This involves the first point, which puts a clear burden of responsibility on the data controller; the second point, because DPbD concerns all the obligations of the GDPR; the third point, since redesign is only required if technically and economically feasible; the fourth point, because it applies to the stages of development and use of PDPSs; and the fifth point, since all data controllers must take appropriate measures.[54] On the one hand, this will raise the cost of developing PDPSs and thus raise the threshold for entering and competing in the markets that involve PDPSs. On the other hand this will create a market for technologies that enable DPbD, and the third point, i.e. the condition of implementing 'state of the art' technologies will stimulate innovation, because new solutions that become 'state of the art' will be in demand. As long as discrimination of particular solutions is based on the extent to which they nourish compliance and not on irrelevant technical details, such discrimination is justified under the compensation objective. The question remains, then, how the moving target of 'state of the art' technical solutions fits with the sustainability of the law.

#### 3.2.3. *As to the sustainability objective*

This is not an easy question. The sustainability objective refers, as we have seen above, to the issue of high-speed adaptations of legal provisions to high-speed developments in PDPs and to the connected issue of legal certainty. Notably, the fifth point refers to 'appropriate' technical and organisational measures. To the extent that the data controller determines what is appropriate it would enjoy a wide margin of interpretation, rendering it questionable whether the aim of the provision can be met. Art. 23.4 and 23.5 might provide a way out here, as well as for the need to envisage high-speed adaptations of the legal framework, by empowering the Commission to issue technology specific regulations, including technical standards, discussed as the sixth point. This could mean that thanks to the delegated acts, DPbD can provide a measure of legal certainty, because it allows for the translation of the sufficiently specific legal conditions of data protection into technical and organisational requirements, which was highlighted as the fifth point. The Commission can

[53] Klitou, 'Privacy by Design and Privacy-Invading Technologies'.

[54] The GDPR allows for joint data controllers (art. 24).

react faster than the EU legislator, thus allowing adaptivity. The expertise needed for more technology specific norms and the ability to negotiate with the stakeholders to develop technical and organisational standards may be a problem for the regular EU legislator, whereas expertise may be solicited or developed by the Commission more easily. But, where the devil is in the details, EU MSs may be right to object to the substantive powers and competences foreseen for the Commission in terms of delegated acts and standard setting. The Treaty of Lisbon has introduced delegated acts as a new way for the Commission to intervene as a legislator, and though the procedures for delegated and implementing acts are surrounded by legal safeguards, the Commission does end up with increased legislative powers.[55] Furthermore, adaptivity and legal certainty may at some point require incompatible solutions; the one asking for flexibility, the other for predictability. As highlighted under point five, DPbD is built on the insight that technical and organisational design matters, but default settings of PDPSs may have major implications that are not obvious and disclosing these implications may not be in the interests of those who foresee them. Though it seems the idea of DPbD is sustainable at the high level of abstraction that informs art. 23.1, its realisation at the level of concrete PDPSs is entangled between the need for adaptivity and certainty on the one hand and the need to engage the right expertise as well as the experience of end users whose data protection rights are at stake on the other.

## 4. Conclusion

The legal obligation of data protection by design (DPbD) is a provocative concept and a challenging obligation. One criticism could be that it violates the technology neutrality of the law, by interfering with technology design instead of merely addressing its usage. In this article we have investigated what is meant by technology neutral law by fleshing out three objectives: the compensation, the innovation and the sustainability objective. They refer to the fact that technologies create different constraints and affordances that generate differential patterns of interaction; instead of suggesting that the default settings of technology design are neutral we find that they have a normative dimension which requires the attention and discernment of the legislator. To explain this we have traced three conceptions of the relation between technology and human action: the substantive view that tends to a deterministic understanding of technology, the instrumentalist view that ignores the normative influence of technologies and emphasises its neutrality, and the relational view that highlights both the instrumental and the normative dimensions of technologies, depending on how individuals, groups and societies integrate and consolidate their usage.

Based on the relational perspective on technology we have examined how the so-called EU Cookie Legislation can be understood as a good or bad example of technology neutral law, testing it against the compensation, innovation and sustainability objectives. This provided the background for an analysis of the novel obligation of DPbD in the proposed General Data Protection Regulation. This obligation targets personal data processing systems (PDPSs) irrespective of whatever technology is used to build and operate them. This analysis discussed six salient points made by the DPbD obligation: first, the choice of the addressee of the norm, being the data controller and not, for instance, technology developers who are not data controllers; second, the fact that this obligation involves the set of rights and obligations outlined in the Regulation and not the less definable notion of privacy; third, the provision articulates two conditions that determine to what extent data protection must be built into the design of PDPSs, notably the technical and economic feasibility; fourth, the provision distinguishes between the phase of deciding on what PDPSs will be invested in and the phase of their actual employment, stipulating that the obligation applies in both phases; fifth, DPbD is described in terms of two types of measures, namely technical and organisational, which should be 'appropriate', highlighting the contextual and dynamic nature of DPbD requirements; finally, sixth, the provision attributes competences to the European Commission to issue delegated Acts and to set Standards to fine tune the general obligation to specific contexts or to ensure interoperability and a level playing field across national and sectorial borders. In the last section we investigated how the proposed DPbD obligation fares with the objectives of technology neutrality, taking into account the six points made in the current articulation of the obligation.

Our conclusion is that there is a need for technology specific legislation to ensure the objectives of technology neutral law, even though this may at first seem a counterintuitive proposition. We find that the obligation to integrate data protection by design combines (1) the need to compensate detrimental effects of personal data processing systems, (2) with a keen eye for a level playing field, which should stimulate innovation and prevent unjustified competitive advantages for existing or specific upcoming technologies, whereas (3) the generic level at which the obligation is formulated aligns with the sustainability objective. Obviously, a number of issues remain. The most salient is the question of whether this obligation should not be addressing technology developers directly. To the extent that basic data protection requirements can be articulated at the level of a personal data processing system, irrespective of its further contextualisation, arguments can be given that the compensation objective may be better served if those who fabricate and sell such systems are targeted. A liability similar to product liability could be constructed.

[55] Delegated acts have general application and can amend or supplement non-essential parts of the concerned legal provision. Implementing acts should ensure uniform implementation but cannot amend nor supplement legal provisions. See the new arts. 290 and 291 of the Treaty on the Functioning of the European Union (TFEU). Cf. EIPA, A. Hardacre and M. Kaeding, *Delegated & Implementing Acts, The New Comitology* (4th edition December 2011), available at http://publications.eipa.eu/en/details/&tid=1839. See art. 86, 87 GDPR: The power to adopt delegated acts can be revoked at any time by the European Parliament (EP) or the Council. Once they have been decided by the Commission they will enter into force unless an objection has been expressed either by the EP or the Council.

**Mireille Hildebrandt** (*Hildebrandt@law.eur.nl.*) *is Senior Researcher at Law, Science, Technology and Society (LSTS) at Vrije Universiteit Brussels, Associate Professor of Jurisprudence at the*

*Erasmus School of Law (ELS), Rotterdam, and holds the Chair of Smart Environments, Data Protection and the Rule of Law at the institute of Computing and Information Sciences (iCIS), Radboud University Nijmegen, Netherlands.*

**Laura Tielemans** *(Laura.Tielemans@vub.ac.be) is doctoral researcher at the Research Group Law, Science, Technology and Society (LSTS) at Vrije Universiteit Brussels, Faculty of Law and Criminology, Brussels, Belgium.*