Co-regulation in EU personal data protection

Kamara, Irene

Published in:
European Journal of Law and Technology

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'

Irene Kamara [1]

Cite as Kamara, I., "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", in European Journal of Law and Technology, Vol 8, No 1, 2017.

ABSTRACT

The recently adopted General Data Protection Regulation (GDPR), a technology-neutral law, endorses self-regulatory instruments, such as certification and technical standards. Even before the adoption of the General Data Protection Regulation, standardisation activity in the field of privacy management and data security had emerged. In 2015, the European Commission issued the first standardisation request to the European Standardisation Organisations to develop privacy management standards based on art. 8 of the EU Charter of Fundamental Rights. There is a rising shift from command-and-control regulation to the inclusion of co-regulation tools in the EU data protection legislation. The aim of this article is to provide insights on the role of standardisation as a form of co-regulation in the data protection context.

Keywords: technical standards; Internet of Things; personal data protection; co-regulation; self-regulation; privacy by design; technology neutrality

1. INTRODUCTION

Discussing privacy governance, Bennett and Mulligan, argue the insufficiency of legislation alone to address privacy challenges. '*Law is necessary, but not sufficient. It needs to be supplemented by other policy instruments, fashioned and implemented within a policy network*' (Bennet, Mulligan, 2002). The authors propose the adoption of a policy 'toolbox' comprising of codes of conduct, privacy impact assessments, privacy standards, privacy seals and other instruments to supplement the law. Several reasons support such argument for shifting from a command-and-sanction regulatory model to a *hybrid co-regulation model* in protection of personal data. [2] Namely, a model that combines both legislation and self-regulatory instruments in support of the law. One argument in favour of such model, lies with the nature of the instruments at hand; technology neutral legislation and technology-specific self-regulation instruments, such as technical standards. Technologies for processing of personal data often imply the need for technology-specific measures, suitable to address the implications of divergent technology effects on the protection of personal data. The EU data protection law is technology neutral legislation: even though it prescribes technology design obligations, the law itself does not specify means to achieve such obligations. Technical standards, on the other hand, may prescribe technical requirements and have faster development processes in comparison to legislation, which in principle enables them to follow and adapt to advancements of technologies. In addition, standards may include quality management requirements for an organisation (such as the ISO/IEC 9001 standard).

Another argument in favour of co-regulatory instruments in the field of data protection law, is the increase of number of organisations processing personal data and their processing capabilities. Command-and-sanction regulation preconditions the enforceability of the prescribed obligations. It is often reported however, that supervisory authorities lack resources to monitor every possible data processing operation in their jurisdiction and, when necessary, enforce legislation. [3] Benett (2010) argues that data protection authorities in their role as accountability agents must be assisted by surrogates, such as standard-setting bodies, accounting firms, and others. Compliance with technical standards, could, under conditions, [4] facilitate the audits of the supervisory authorities, by providing a first point of reference.

The above reflections have been supported by both practitioners and the legislator. Standardisation activity has increased in the field of personal information protection. In 2014, the cloud computing technical standard on the protection of personal information was published by ISO and IEC. [5] In terms of legislation, the General Data Protection Regulation has brought self-regulation efforts in the spotlight. [6] The GDPR encourages the use of codes of conduct, data protection certification mechanisms, data protection impact assessments, and technical standards to promote transparency and compliance with the law. [7]

In 2015, the European Commission issued a standardisation request to the European Standardisation Organisations to develop privacy management standards ('mandate'). The mandate, which is a Commission Implementing Decision, is the first standardisation request based on the fundamental right of protection of personal data as enshrined in art. 8 of the Charter and art. 16 of the Treaty on the Functioning of the European Union (TFEU).

The aim of this contribution is to provide insights on standardisation as a form of co-regulation in the data protection context and draw preliminary conclusions on a potential role and limitations of standardisation in relation to (data protection) law. The article is structured in two main parts. The first part introduces European standardisation as a form of regulation.

It analyses the concepts and types of self- and co-regulation and offers insights on how standardisation fits under those concepts. The second part provides a deeper analysis of European standardisation as a co-regulation tool, by studying the European Commission standardisation request in the field of data protection. This part delves into challenges stemming from emerging and developing technologies posed to the protection of personal data, but also the juxtaposition of the technology neutral nature of the EU data protection legislation (GDPR) with its technology design provisions. This discussion provides the background for the analysis of the standardisation request on privacy by design and by default. Finally, the last section draws conclusions and highlights promises and pitfalls of standardisation in the field of personal data protection.

2. SELF-REGULATION: CONCEPT 'MAPPING'

2.1. DEFINING SELF-REGULATION

In several fields non-legislative instruments have a prominent role in the governance of a series of issues, either by assisting legislation or in other ways existing in parallel with the legislation. What is broadly called 'self-regulation' encompasses a broad range of instruments, such as codes of conduct, technical standards, certification, seals and trust-marks. The term itself is defined in many ways and there are different approaches to self-regulation. Defining first in a negative manner, self-regulation is non-legislative. Laws are developed and put in force with specific procedures in every state or international level through treaties and agreements, with the involvement of authorities, government and a body of electorates with legislative powers, applicable to its people and enforced by judicial decision. Price and Verhulst (1999) in search for a definition of self-regulation compare it to *de-regulation* and *non-regulation*. They argue that de-regulation directly aims to remove any regulation perceived to be excessive and to hinder market forces. Self-regulation on the other hand, 'does not aim primarily to dismantle or dispense with a framework for private activity, but rather to change the actor who establishes this framework'. In relation to non-regulation, the authors assert that self-regulation is no alternative or substitute for elements of direct regulation.

The term self-regulation includes two elements that need to be defined: 'self' and 'regulation'. Additionally, since self-regulation cannot replace law and state powers, it is necessary to identify the relation of self-regulation to the state.

Black argues that 'self-regulation describes the situation of a group of persons or bodies, acting together, performing a regulatory function in respect of themselves and others who accept their authority' (Black, 1996, p.27). Thus, the 'self-' refers to an association of persons or bodies that act together. The collective group does not regulate only themselves, but also other persons or entities accepting their authority. As a result, the audience of a European standard for example, drafted by the CEN Technical Committee on air quality, is broader than what the 'self-' element reflects, that is the participants of the committee. Once the European standard is available to the public, any organisation that wishes, is free to comply with the standard. Collectiveness in both the group performing the self-regulatory action and the audience is better depicted when one contrasts individual self-regulation to collective self-regulation (Price and Verhulst, 2000). In the former concept, an entity regulates itself, independent of others, while in the latter, a group is regulated.

The term 'regulation' (in 'self-regulation') refers to the rule-making capacity of the self-regulatory group or entity. Such rules can be expressed in a variety of instruments. The relation of the state to self-regulation leads to further categorisation into 'sanctioned', 'coerced'

and 'voluntary' (Black, 1996). Particular interest for the technical standardisation case in the field of personal data protection presents the *sanctioned* and *voluntary* self-regulation. Sanctioned self-regulation implies that the outcome of the self-regulatory effort is pending approval from the state, while voluntary is independent from any state involvement. Usually, there are more models in between, demanding more or less state involvement or endorsement. An example is co-regulation. [8] Hirsch (2011) notes that in co-regulation, government and industry share responsibility for drafting and enforcing regulation. The legislator sets general pillars of the legal framework, but eventually the government remains involved in the self-regulatory initiatives at least in a monitoring function supervising the progress and the effectiveness of the initiatives in meeting the perceived objectives (Weber, 2010).

2.2. LEGAL EFFECTS, BENEFITS AND DRAWBACKS OF SELF-REGULATION

Following the diversity in definitions of self-regulation, the effects of self-regulation rules are also diverse. The rules might have legislative power, contractual effect or no legal status at all (Black, 1996). Bonnici (2007) draws three criteria associated with state rules in order to examine in each case the legal effect of self-regulation rules. The first criterion is the *binding effect* of the rules. Whether a rule has a binding effect can be assessed by the intention of the developers of the rule (for instance expressed in an explicit statement) and the existence of sanction mechanisms for non-conformity with the rule. Another criterion is the *transparency* of both the rules and the rule-making process. The legal effect of the self-regulation rules is possible only if the rule itself and the development process are known in advance to the intended audience. The third criterion, according to Bonnici (2007), is *legal certainty* by means of clarity, stability and public nature of the rules.

Self-regulation has advantages in relation to command-and-sanction regulation. Flexibility and adaptability to new technological needs are two of them. Self-regulation is viewed as 'consistent with innovation and consumer-oriented, contextual responses to privacy concerns' (Bennet and Mulligan, 2012, p.1). The fact that self-regulation involves market stakeholders makes its instruments more easily welcomed and adopted by those stakeholders, as it promises to accommodate their needs. However, some of the above characteristics might also pose challenges to the consumers/individuals and stakeholders such as Small-Medium Enterprises (SMEs). The rights of the individuals and those stakeholders might be not sufficiently protected by industry-led self-regulatory initiatives. Self-regulation, in the sense of individual and collective self-regulation, does not officially involve formal governmental approval (Priest, 1997-1998). Benett and Raab (2006) explain that self-regulation tends to be more lenient than government requirements, and may not achieve public goals. Also, from a business perspective, Hirsch highlights that 'without the ability to guarantee legal compliance, pure self-regulation will neither attract sufficient industry involvement nor address the need for international privacy standards' (Hirsch, 2013, p. 1043). When it comes to disadvantages, scholars make a distinction between individual and collective self-regulation on the one hand and co-regulation on the other hand (Hirsch, 2013). The distinction is justified by the element of regulatory oversight, which exists in varying degrees and scalability in co-regulation, but is absent in individual and collective self-regulation. The European Commission highlights that co-regulation allows 'the parties involved to define implementing measures in accordance with the objectives defined by the legislator' (European Commission, 2001).

3. EUROPEAN STANDARDISATION AS SELF- AND CO-REGULATION

3.1. LEGAL FRAMEWORK AND STANDARDS' TYPES

The legal framework on the organisation of European Standardisation is Regulation 1025/2012. The Regulation establishes rules for cooperation among the European Standardisation Organisations, [9] national standardisation bodies and rules on the European standards and European standardisation deliverables (art.1). A ' *standard means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory (..)* ' (art. 2 1025/2012 Regulation). European standardisation is based on fundamental principles, as provided in the Regulation 1025/2012, namely coherence, openness, transparency, consensus, voluntary application, independence from special interests and efficiency, even though their regulatory enforcement has been criticised (Van Gestel, 2013, p.177).

The Regulation lists in an exhaustive manner the types of standards under its scope [art. 2(1)], namely international standards, European standards, harmonised standards and national standards. Taxonomies of standards vary: [10] CEN and ISO make a distinction between standards which include requirements and/or recommendations in relation to products, systems, processes and services. There is also a distinction between standards which describe a measurement or test method or establish a common terminology within a specific sector. [11] Wurster et al. categorise standards to fundamental standards, analysis and trial standards, performance standards and organisational standards (Wurster, 2015). Gleeson and Walden (2014, p.8) categorise standards in three types; technical, informational, and evaluative. Technical standards specify details for 'format, protocol, or interface and describe how things work in an interoperable manner'. Informational standards are the specifications that provide guidance and information to organisations about a product or a service. Evaluative standards test and certify the proper use of best known practices. Gleeson and Walden argue that conformity with technical standards can be measured objectively, while evaluative standards necessitate third-party audit.

R.1025/2012	ISO/CEN	Walden and Gleeson	Wurster et al.
International	Requirements Standards	Technical standards	Fundamental standards
European	Recommendations Standards	Informational standards	Analysis standards
Harmonised	Requirements/recommendations standards	Evaluative standards	Trial standards
National	Common terminology	-	Performance standards
	Measurement	-	Organisational

Table 1: Types of industry-led standards [12]

3.2. EUROPEAN STANDARDS AS COLLECTIVE SELF-REGULATION?

European standards (EN) are voluntary. The voluntary nature refers to the choice of an organisation to comply with the standard. Manufacturers, service providers, and other economic operators, or conformity assessment bodies may choose another technical solution to demonstrate compliance with the mandatory legal requirements. [13] However, once the entity complies with a standard, this entails certain obligations for that entity. Such obligations aim mainly to ensure the uniform application of the standard among the entities that claim to comply with the standard and offer transparency towards the consumers as to what compliance with the standard entails. Moreover, in terms of liability, the standards may have legal effects. Once a party chooses to apply a standard, there is usually a presumption of compliance established, meaning that such party is presumed to comply with the requirements set in the standard, which in turn are expected to be lawful themselves (De Hert et al., 2016). Thus, compliance with standards may create 'legitimate expectations' and people may assume them to have official legal standing (Falke et al., 2000).

The voluntary nature of the standards in combination with the fact that they are usually market-driven (Rec. 11 Regulation 1025/2012) justify their characterisation as self-regulation. European standards could be in principle characterised as an instrument of *collective self-regulation*. [14] Standards are best practices, that can be applied not only by the entities that participated in the development process (through the national delegations), but any entity that can be benefited by applying the EN and indirectly acknowledges the rule-making capacity of the standardisation organisation by complying with the EN. In that sense, the 'collective' element of the collective self-regulation is fulfilled.

3.3. STANDARDISATION REQUESTS ('MANDATES') AS CO-REGULATION

Even though in principle standardisation qualifies as collective self-regulation, there are exceptions to this argument. An exception is established in the case of standardisation requests issued by the European Commission and addressed to the European Standardisation Organisations. The aim of such requests is to establish 'an agreed way of meeting legal requirements on health, safety, environmental protection, civil security and interoperability' and to 'promote technical development' (European Commission, 2015). A standardisation request may be issued in support of a *Union policy* or *Union legislation*.

The process is defined in art.10 of the 1025/2012 Regulation. The European Commission drafts a request for the European Standardisation Organisations describing the policy goals, the legislation and the need for standardisation in a field or topic. The 'mandate' also includes the type of requested deliverables and the objectives that need to be accomplished. From a legal perspective, the standardisation request is a Commission Implementing Decision based on the Regulation 182/2011. [15] The European Standardisation Organisations may accept or reject the request within a month from the receipt. If accepted, the standardisation request is a legally binding contract for both sides (Schepel, 2005). This form of regulation involves regulatory oversight in several stages: the Commission may participate as an observer in the meetings of the Technical Committee carrying out the standardisation work in line with the mandate. Also, the Commission approves the Workplan the Technical Committee prepares before starting the development of the deliverables. The European Standardisation Organisations maintain their independence in terms of the content of the deliverables and

administration, which corresponds to the market-driven approach of co-regulation. [16] The technical standards resulting from the standardisation request, fit the description of *co-regulation*, as there is involvement of the regulator in the standardisation process, but also the flexibility of the European Standardisation Organisations as to the type and content of the standardisation deliverables.

4. STANDARDISATION AND THE EU DATA PROTECTION LEGISLATION

Following the 'constitutionalisation' of the right to data protection (De Hert, Gutwith, 2009), in 2012, the European Commission proposed a General Data Protection Regulation, with the aim to reform and modernise the legal framework on Data Protection in the European Union (European Commission, 2012). The first reading at the European Parliament introduced a series of important amendments to the Commission proposal in 2014 and later in 2015 the Council reached a general approach on the proposal for the legislation. [17] In May 2016, the General Data Protection Regulation was published in the Official Journal of the EU.

The first assessments in 2012 were that the Commission 'took bold steps for the improvement of the data subjects' position in contemporary personal data processing conditions' (De Hert, et al. 2012). Indeed, the GDPR includes substantial novelties in relation to the previous regime of the Directive 95/46/EC (De Hert, et al. 2012). However, the sufficiency of the new legal provisions alone to regulate the emerging technologies is still to be seen after the General Data Protection Regulation is applicable in 2018.

As a general remark, independently of whether and how the new Regulation will meet its objectives, its capabilities as a legal instrument are within the framework of capabilities of any legal act. The prescription of obligations and principles need to fulfil requirements such as predictability and foreseeability (Cox, 2006), formal legality (laws must be set forth in advance, they must be general, they must be publicly stated, they must be applied to everyone according to their terms, and they cannot demand the impossible) (Tamanaha, 2012).

The GDPR includes a spectrum of different provisions modernising the Data Protection Directive provisions. As in the 95/46/EC Directive, the GDPR endorses Codes of Conduct. [18] Additionally, the GDPR acknowledges the importance of other 'self-regulatory' tools, such as standardisation and certification (art. 42, 43 GDPR). The endorsement of such measures by the GDPR provides the basis for the potential role of self-regulation in support of Union legislation.

The GDPR refers to technical standards [19] not only as a general *good practice* approach, but as means of *transparency* to the data controller's practices and *compliance* with the legislation. Standardisation (and certification) are endorsed in relation to the new modalities and tools introduced in the GDPR, such as data protection by design and by default art. 25 GDPR. The preparatory works and the final text of the GDPR differ substantially in terms of the provisions explicitly referring to standardisation. The final text of the GDPR mentions technical standards in art. 43 GDPR and art. 22 GDPR. In the European Parliament First Reading version (2014), standardisation was included in provisions on standardised information policies (art. 13a of European Parliament First Reading), provision of information to the data subject (art. 14 of European Parliament First Reading), exercise of the right to object (art. 19 (2b) of European Parliament First Reading), and data security processing of personal data concerning health (art. 81 of European Parliament First Reading). The omission of the

direct reference to technical standards is a legislative choice that allows for more flexibility in the standardisation activity in the field. First, the choice to avoid references to Commission standardisation allows for flexibility on the subject-matter of the standards to be developed. Second, this choice allows both the standardisation bodies and the European Commission to initiate and carry out the standardisation activity. The Vademecum on European Standardisation in support of Union Legislation and policies (2015), which is the policy document aiming to explain the Commission's role in standardisation requests, provides that technical standards or technical rules cannot be developed for subject matters, for which *the legislation provides* they are adopted by a Commission delegated or implementing act.

Article 22(5) provides the possibility to the data subject to exercise the right to object to processing concerning him or her, including profiling, with automated means using technical specifications. A relevant technical specification in this case would be the Do Not Track standard which is being developed by the W3C, the World Wide Web Consortium (Kamara, Kosta, 2016). The other provision explicitly relating to standards, is art. 43(9) GDPR, which provides that the Commission has the power to adopt implementing acts laying down technical standards related to certification mechanisms, data protection seals and marks. Standardising requirements of the evaluation, auditing process and recognition of certifications across the Member States, would result in higher degree of harmonisation. Apart from the explicit reference to standardisation in art. 22 and 43 GDPR, several provisions of the GDPR could be the basis for development of technical standards in the field. One prominent example is the provisions that establish *technology design obligations*, such data protection by design and by default (art. 25 GDPR) as we further explain in the following sections.

5. THE COMMISSION PRIVACY BY DESIGN STANDARDISATION REQUEST TO THE EUROPEAN STANDARDISATION ORGANISATIONS

In 2015, the European Commission published its decision on a standardisation request ('mandate') towards the European Standardisation Organisations (ESOs) (European Commission, 2015). The mandate concerns deliverables for privacy and personal data protection [20] management in support of Union's security industrial policy. Prior to the standardisation request, stakeholders were consulted, such as the European Data Protection Supervisor and ANEC, the consumer protection association in standardisation. Before analysing the content of the mandate, it is interesting to explore reasons that implied the need for standardisation activity in the field.

5.1. BACKGROUND

5.1.1. EMERGING TECHNOLOGIES AND INCREASING CHALLENGES: INTERNET OF THINGS

Notwithstanding the benefits of technology innovation to the individuals, the digital economy, and society (European Commission, 2013), pervasive technologies which track the activities of the user across the Internet, interconnect data, and compile user profiles pose a constant challenge to the fundamental rights to personal data protection and privacy (Kamara, Kosta, 2016). Citizens in public and semi-public areas are often recorded with high-resolution and increased-capability surveillance systems, analysing patterns in behaviours, external characteristics, and facial expressions. [21] Technological advances and the use of technologies may in general pose relevant privacy and data protection risks, but emerging technologies in

particular, render it significantly challenging for the law to anticipate the impact of such technologies on the fundamental rights to private life and protection of personal data.

For the purposes of this article, emerging technologies are 'science-based innovations with the potential to create a new industry or transform an existing one' (Day et al., 2004). Characteristics attributed to emerging technologies are: [22] 1. The fast rate of evolution of products, systems and processes; 2. The convergence of technologies, which denotes creative combinations of new and old technologies, new and old methods of production, and business models and 3. Network effect [23] (Srinivasan, 2008).

We take a broad example of Internet of Things to illustrate the inherent data protection, security and privacy risks of such technologies. [24] Internet of Things is 'an infrastructure in which billions of sensors embedded in common, everyday devices - 'things' as such, or things linked to other objects or individuals - are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities' (Article 29 Data Protection Working Party, 2014, p.4). Internet of Things may, therefore be considered as emerging technology in the above sense, as it has been an innovation which created a whole new market for devices, software and hardware components that interconnect to each other. Examples of Internet of Things (IoT) technologies are home automation devices, such as thermostats connected with CCTV, digital locks activated via smartphones, self-parking cars and others. [25]

The Article 29 Data Protection Working Party (2014) stresses the risk of lack of control and information asymmetry. [26] The function of IoT requires data collection and transmission among devices, objects and systems. Data are automatically generated for instance via the sensors of smart devices, and collected. This activity may result in non-effective exercise from the individual of the data protection rights of information, access, rectification and erasure of the data and the risk of excessive self-exposure is possible. Another risk is related to data security. Heterogeneity might affect the degree of infrastructure protection (Roman et al., 2011). Confidentiality, availability and data integrity measures are required to mitigate the risks of data security breaches. Given the complexity of IoT networks and the number of stakeholders involved in different functions and processes (storage infrastructure, communication links and others) mitigation of such risk might be overly challenging (Article 29 Data Protection Working Party, 2014). Ziegeldorf et al. (2014) argue that the threat of identification is one of the most dominant, given that facial databases become available to marketing platforms, but also speech recognition use in mobile applications. As the Article 29 Data Protection Working Party notes (2014) 'wearable things kept in proximity of data subjects result in the availability of a range of other identifiers, such as the MAC addresses of other devices which could be useful to generate a fingerprint allowing data subject location tracking.'

The above risks, provided here by means of example, are related to the types and capabilities of the technologies involved in the collection, use and processing of the personal data and information. Technologies might increase existing data protection risks or introduce new risks, especially considering the fast rate of evolution and convergence of emerging technologies. The personal data and privacy challenges stemming from the rapid development of emerging technologies raise the need for regulation, which can achieve protection corresponding to the specific risks.

5.1.2. TECHNOLOGY NEUTRALITY IN THE DATA PROTECTION LEGISLATION

The GDPR follows the principle of *technology neutrality*. The essence of a technology neutral law is that the law does not discriminate between technologies if the rationale behind the legislation would apply equally to each technology (Moses, 2007). Hildebrandt et al. (2013) identify the following as one of the objectives for a technology neutral law:

> '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.'

Moreover, technology neutral legislation does not force the use of one technology where an equivalent alternative technology is available (Moses, 2007). Reed (2007) adds one more layer to technology neutrality by arguing that 'the fundamental rules should be the same online as off-line', even though he largely contests this approach for its ambiguity. The so called ' *online and offline equivalence*' means the law applies 'to the behaviour of the actors involved and the effects of that behaviour and not to the means through which the actors behave or by which those effects come about' (Reeds, 2007). [27] A technology neutral law is distinct from a *technology indifferent* (or else independent) law. [28]

In the context of the General Data Protection Regulation, the principle of technology neutrality implies that the protection of individuals should not depend on the techniques (and technology) used for the processing of personal data. [29] A technology neutral law in the sense of the General Data Protection Regulation is likely to avoid risks of circumvention, namely that the circumventer uses a different technology than the one forbidden by the law, resulting in equivalent harmful interference with the individual's data.

In a study prepared for the UK Information Commissioner's Office, the principle of technology neutrality of the Data Protection Directive 95/46/EC is considered as strength (Robinson, 2009). Indeed, among the benefits of such an approach is future-proof legislation; technological neutrality aims to 'avoid uncertainty, poor targeting and obsolescence as the technological context evolves' (Moses, 2007). The European Data Protection Supervisor also warns that failure for the European legislator to develop a future-proof data protection framework could render some of the rules 'ineffective' (Moses, 2007). Legislation should not seek continuous adaptation to emerging technologies, as the 'procedure for legislative acts takes too much time to be effective in 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' (Hildebrandt, 2007). In the example of anonymisation in an IoT network, a technology-specific (as opposed to technology neutral) regulation would either endorse specific measures such as types of anonymisation techniques; or prohibit the use of other technologies that are for example found to be vulnerable to attacks and raise therefore issues of data security. In both cases, the law would give rise to questions regarding its sufficiency. In the first case, the endorsement on the use of a specific technology would at some given point in the future be out-dated. This could in turn lead to the paradox of controllers complying with the law, but not safeguarding the data subjects, at least until the law would be amended. In the second case, the vulnerability of a technology might be reversible and improved over time, thus a law that prohibits a specific technology would be obsolete. [30]

As Koops notes (2006), it is the *effects* of technology *use* and potentially the *functions* of technologies that should be regulated, instead of the technology itself. This is a good starting point for a law that cannot be indifferent to technological advance but cannot either be technology specific for the reasons explained in this section. Nevertheless, even the effects and the functions in case of emerging technologies might not always be foreseeable. A prominent example is the Data Protection Directive of 1995 and technologies such as wearable devices collecting images and sounds (personal data) or self-driving cars.

Since technology neutrality has significant advantages in the case of data protection legislation, the question of how to deal with the specific technological challenges remains to be explored.

5.1.3. TECHNOLOGY DESIGN OBLIGATIONS IN THE GDPR: DATA PROTECTION BY DESIGN

The technology neutral General Data Protection Regulation prescribes technology-related obligations. Art. 25 GDPR introduces Data Protection by Design (and Data Protection by Default). Data Protection by Design seeks for technical solutions to address privacy and data protection requirements defined in the EU data protection legislation (Tsormpanoudi et al., 2016). The (broader) concept of Privacy by Design [31] stems from the value sensitive design scholarship, and the core idea is the implementation of privacy principles and requirements 'into the design, operation and management of information processing technologies and systems' (Costa and Poulet, 2012).

The GDPR in its art. 25(1) provides that the data controller shall implement technical and organisational measures appropriate for the protection of the data subject rights not only at the time of processing of personal data, but also when determining the means of processing, thus at an earlier stage. Furthermore, 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, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.' [32]

Another example of a technology design obligation is the right to data portability (art. 20 GDPR). The right to data portability, entails the right of the data subject to receive the personal data concerning him or her from the data controller in a structured and machine-readable format, and the right of having the personal data transmitted to another controller. Data portability responds to an actual practice of companies retaining personal data in non-interoperable formats, which results in hindering individuals from changing service provider (vendor lock-in). The right to data portability implies the obligation of the data controller to keep the data in an interoperable format. A previous version of the GDPR article (art. 18§3 of the European Commission proposal, 2012) explicitly provided the Commission with the power to specify the type of electronic format and the technical standards, modalities and procedures for the transmission of personal data. In the final GDPR version, such power is not explicitly delegated to the Commission, however data portability and interoperability are an important standardisation field. [33]

The GDPR, despite its technology neutral nature, implies technology-related obligations, as in art. 25 and 20 GDPR. However, the legal obligations maintain a level of normative abstraction, which necessitates further elaboration, with instruments that can be technology-specific and context-specific.

5.2. MAIN ELEMENTS OF THE PRIVACY BY DESIGN STANDARDISATION REQUEST

Following the prominent issues for dealing with technology specific risks and the need for elaboration of technology design obligations, the European Commission - while the EU data protection legislative reform was pending - issued the Commission Implementing Decision on standardisation in the field of data protection and security policy (mandate).

The mandate was issued in support of the Data Protection legislation and the Security industry policy of the Union. The Data Protection Directive 95/46/EC and the Commission's proposal for a General Data Protection Regulation form the legal basis of the mandate. [34] The mandate is addressed to CEN, CENELEC and ETSI, with a request for collaboration in order to carry out the mandated work. With regard to the expected deliverables, there is a request for two types of deliverables, namely European standards (EN) and standardisation deliverables that will guide the manufacturers and service providers on how to realise the targets of the EN. The number of the standards and other deliverables will be determined by the ESOs.

In specific, the requested standardisation activities are the following:

(1) One or more European standards on how to address and manage privacy and personal data protection issues during the design and development and the production and service provision processes of security technologies and services, allowing manufacturers and service providers to develop, implement and execute a widely recognised 'Privacy by Design' (PbD) approach in their processes.

(2) One or more related European standardisation deliverable(s), addressed to the manufacturers of security products or systems and service providers when specifying the privacy and personal data protection management processes with an explanation how to realise them, including descriptions of the necessary roles, tasks, documentation, hardware and software requirements, and templates to be used when applying the requested standard(s).

The request was accepted by the ESOs, which established the Joint Working Group 8 (JWG8) with the aim to conduct the standardisation request. [35] Notwithstanding the significance of the future deliverables, which may contribute to compliance with the data protection legislation, one should note the importance of the mandate itself.

The mandate is the first European Commission standardisation mandate in support of the right to protection of personal data on the basis of art. 8 of the Charter, art. 16 TFEU and the data protection legislation. Previously, there have been mandates such as the M/436 on Information and communication technologies applied to Radio Frequency Identification (RFID), which may include privacy aspects but not as the main focus of the standardisation activity. In addition, there have been standardisation activities related to privacy management and information security mainly at international level. Prominent examples are the ISO/IEC 27000 series, which includes standards for information security risk management, the

ISO/IEC 29000 series on Privacy framework and Security Techniques in Information technology and the ISO 22307 on Privacy Impact Assessment in the Financial Services. Moreover, those standards are not built on the basis of the European legislation and do not claim compliance with the Union law.

This first co-regulation effort in the field of data protection has an envisaged added value in terms of serving policy objectives and public interests, but also support the Union legislation on the protection of personal data, as is further discussed in the following section.

5.3. THE PRIVACY BY DESIGN STANDARDISATION REQUEST AS THE FIRST TEST FOR CO-REGULATION IN THE REFORMED EU DATA PROTECTION LANDSCAPE?

The mandate directly acknowledges the significance of European standardisation to support the data protection legislation. The added value of the standards in data protection and privacy requirements in the design of security products is envisaged in the management process organisations. Organisations that process personal data may use privacy management processes to facilitate compliance with the principle of accountability. A standard may provide an indication to organisations, per the mandate, on how to prepare, implement, monitor and revise the management process for privacy and data protection issues. Such privacy management processes need to be implemented in each step of the design, development and production/service provision of security technologies and services. The mandate also provides that requested standard (s) are expected to promote compliance with the data protection legislation.

The mandate itself is the first test for co-regulatory measures in the EU data protection field based on art. 8 of the Charter. Apart from endorsements in the GDPR, the standardisation request takes the legislator approach one step further into operationalising the endorsement with a concrete request for technical standards in the field. The European Commission took steps into signalling the significance of technical standards by asking the European Standardisation Organisations to draft standards that develop, implement and execute a 'Privacy by Design' approach.

The following elements stand-out in this co-regulation initiative in the field of personal data protection:

- Initiator of the activity. The mandate is initiated by the European Commission, not the industry or another actor. Thus, a public authority requested the development of a self-regulatory instrument in the data protection field (co-regulation).
- Degree of regulatory involvement. The regulator did not only endorse standardisation activity in the field, but issued a specific request to the ESOs for the development of European standards in the field with predefined goals. [36] Throughout the development process the regulator (European Commission) participates as an 'observer', without voting rights, but following the progress of the standardisation work.
- Relation to data protection legislation. The standardisation request was issued in support of Directive 95/46/EC of the European Parliament and of the Council. The GDPR was finalised in 2016, over a year after the adoption of the mandate (which explains why the request refers to the Directive in its title, instead of the GDPR). However, the text makes references also the Commission proposal for a General Data

Protection Regulation (2012). Most importantly, the mandate refers to the art. 8 of the Charter of Fundamental Rights of the EU and the art. 16 (1) of the Treaty on the Functioning of the EU. Therefore, there is a reference to personal data protection, not only as a legal instrument, but as a fundamental right.

- Target audience. The EU data protection legislation establishes legal obligations for the data controllers, the natural or legal person that determines the means and purposes of the processing activity. [37] In the security market, the controller is the customer of the security products or systems, for instance surveillance cameras. However, the data protection by design approach cannot be implemented by the customer, but the manufacturer of the product or system. The latter however is not subject to the data protection legislation, as the manufacturer is not involved in the processing of personal data, which takes place once the system is installed or the product in use. The standardisation activity aims to address this paradox [38] by developing data protection by design standards for the manufacturers to implement. [39]
- Function of standardisation. The aim of the requested activity is to provide voluntary tools to manufacturers and service providers to allow them to demonstrate to controllers using or utilising their products and services that their products and services have been designed and developed duly respecting data protection by design and default. [40]

Overall, the standardisation request illustrates an envisaged added value of technical standards to the protection of the fundamental right to personal data protection. The Commission has stressed the added value of standardisation in addressing complexities of (security) technologies. Standards are expected to specify 'how legal instruments will be implemented'. The added value lies among others in one of the goals of the standardisation work based on the mandate that is to translate the concept of 'Privacy and personal data protection by Design' into concrete indications for manufacturers and service providers to plan, implement, control and revise a management process.

Since the standardisation work is ongoing, the deliverables, their suitability, quality and compatibility with the EU data protection law and principles, are to be assessed ex post, once the European Standards and other deliverables are finalised. [41] Nevertheless, points of criticism concern terminological issues, the timing for issuing the standardisation request, and the choice of the subject matter. Apart from the terminological inconsistency with the GDPR ('privacy by design and by default' instead of 'data protection by design and by default'), the timing to issue the request, namely while the EU data protection reform was ongoing, raises questions. It resulted in a mandate which is mainly based on the Data Protection Directive 95/46/EC instead of solely on the General Data Protection Regulation, which was adopted one year after the adoption of the Commission Implementing Decision. Even though the Working Group developing the standards based on the mandate, will probably consider the new legislation instead of the repealed one (the Directive), the text of the mandate confusingly refers to both legal instruments. Regarding the subject matter of the mandate, as Privacy by Design is a concept that has not yet crystallised or found widely-accepted implementation, it is not a suitable subject matter for standardisation at the moment. This may result to further implications in relation to the quality and acceptability of the standardisation deliverables.

6. CONCLUDING REMARKS: THE FIRST 'TEST', PROMISES AND PITFALLS

Technologies emerge with rhythms that were inconceivable a few decades ago. The impact on the life of individuals has long been discussed and will probably continue to be discussed and analysed. The emergence of several technologies has also an impact on law. The law needs to adapt and transform in order to serve its role, protect the citizens and the society. The capability of the adaptability of the law might reflect on the serving of its goals; an outdated law unable to keep-up with new challenges, new ways of committing crimes, new concepts that do not fit the definitions of existing provisions, new threats to the protection of rights.

However, what are the limits to such adaptability? Taking the example of personal data protection legislation in the European Union, we can derive certain characteristics of (secondary) law. Apart from the various constitutional and other limitations set by treaties and other primary law, the law is limited by its very inherent characteristics: it needs to have a level of abstraction, to be futureproof and technology neutral (with some exceptions). Legal provisions are norms; prescribing rules on what one should or not do in a given context under given or implied conditions. A very detailed, or even exhaustive law, which aims to address any possible risk or threat, is vulnerable. A prescriptive law is susceptible to human omission (the one of the legislator) and future challenges. In parallel, a law that is not technologically neutral, but its prescriptions depend on techniques and specific technologies, will inevitably become either obsolete -when new technologies are developed -, allow for circumvention of its provisions (with a different technique than the one mentioned in the law) or will create a legal gap by regulating some of the existing technologies and not some others. Especially in the case of personal data protection, the neutrality of the current and new legislation is justified for several reasons, one of them being the multiple and rapidly increasing risks stemming from emerging technologies. However, there is a need for a set of flexible rules specifying requirements for the protection of the right, but with another instrument than the data protection law.

In this article, we examined self-regulation. Self-regulation appears in several forms, definitions, uses and impacts. Despite the diversity of the self-regulatory landscape and practice, self-regulation as a concept has several characteristics that can be regarded as benefits in relation to the challenges of emerging technologies. Such characteristics include the flexibility and adaptability of the self-regulatory rules. On the other hand, the lack of state authority involvement entails potential threats to the protection of fundamental rights, as there is often no oversight and enforcement by public authorities. In this paper, the example of standardisation mandates provided an example of self-regulation prescribed by law.

The mandate on privacy by design in security products and services illustrates mainly two things. The first is that requirements on technological measures and methods, which cannot be included in the data protection law, maybe be incorporated in technical standards. As the Privacy Bridges project identified, technical standards in the field of data protection may be implemented in several fields such as user controls and the development of easy-to-use mechanisms for expressing individual decisions regarding user choice and consent, transparency, de-identification of personal data and others (Bridges, 2015). Consequently, one could say that emerging technologies created the regulatory need for self- and co-regulatory instruments such as technical standards in the field of personal data protection.

The second lesson from the ongoing standardisation request is that self-regulation has limitations. As mentioned earlier, self-regulation is flexible and market-driven. These characteristics might lead to results that promote the interests of groups that participate in the standardisation activity. In order to ensure that the complementary self-regulation measures protect the rights of the data subjects, regulatory oversight is necessary. Supervision should not limit the independence of the self-regulatory body, in this case the ESOs, but safeguard that the self-regulatory instrument serves its purpose of facilitating protection of the rights in an equal and fair way. Another limitation is overestimating the added value of such instruments in the field of data protection. One should consider the limitations of standardisation, along with its added value. Standards are not law and cannot replace the law. Also, standards have a limited specific scope. Therefore, the data controller or processor cannot fully rely on achieving compliance with the EU data protection law only through standardisation.

Bearing in mind its limitations, standardisation may be a useful instrument to assist compliance with the data protection legislation, especially in relation to the risks created by emerging and rapidly developing technologies.

BIBLIOGRAPHY

Books & Reports

Article 29 Data Protection Working Party (2014) 'Opinion 8/2014 on the on Recent Developments on the Internet of Things', WP 223

Article 29 Data Protection Working Party (2015) Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, WP232

Bonnici Jeanne Pia Mifsud (2007) Self-Regulation in Cyberspace (T.M.C. ASSER PRESS)

Cox Noel (2006) 'Technology and Legal Systems' (Ashgate)

Day, George S., Paul JH Schoemaker, and Robert E. Gunther (2004) 'Wharton on managing emerging technologies' (John Wiley & Sons)

ENISA (2015) 'Privacy and Data Protection by Design'

European Commission (2013) 'Doing business in the digital age: the impact of new ICT developments in the global business landscape Europe's vision and action plan to foster digital entrepreneurship', Study prepared from Deloitte

European Data Protection Supervisor (2015), 'Leading by example, the EDPS Strategy 2015-2019'

Falke, J. and Schepel, H. (eds.) (2000) Legal Aspects of Standardisation in the Member States of the EC and of EFT', (H. S. A. Luxembourg: Office for Official Publications of the European Communities)

Privacy Bridges (2015) 'Report, EU and US privacy experts in search of transatlantic privacy solutions', Amsterdam/Cambridge

Schepel, Harm (2005) The constitution of private governance: Product standards in the regulation of integrating markets (Vol. 4) (Hart Publishing)

Yoffie, David B. (1997) Competing in the age of digital convergence (Harvard Business Press)

Journal articles & Book chapters

Black Julia (1996) 'Constitutionalising self-regulation, The Modern Law Review, Vol. 59, No. 1 (Jan., 1996), 24-55

Colin J. Bennett & Charles D. Raab (2006) 'The Governance of Privacy: Policy Instruments in Global Perspective' 155

De Hert, Paul, and Vagelis Papakonstantinou, V. (2011) 'The Amended EU Law on ePrivacy and Electronic Communications', The John Marshall Journal of Computer & Information Law, 2011, 29-74

De Hert, Paul, Vagelis Papakonstantinou, and Irene Kamara (2016) 'The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection' Computer Law & Security Review 32, no. 1: 16-30

De Hert, Paul, and Serge Gutwirth (2009) 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action' In Reinventing data protection? 3-44 (Springer Netherlands)

De Hert, Paul, and Vagelis Papakonstantinou (2012) 'The proposed data protection Regulation Replacing Directive 95/46/EC: A sound system for the protection of individuals' Computer Law & Security Review 28.2: 130-142.

Gleeson N., Walden I. (2014) 'It's a jungle out there? Cloud computing, standards and the law, in European Journal of Law and Technology, Vol 5, No 2

Hildebrandt, Mireille, and Laura Tielemans (2013) 'Data protection by design and technology neutral law' Computer Law & Security Review 29.5: 509-521.

Hirsch, Dennis D. (2013) 'In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct' Ohio St. LJ 74: 1029.

Hirsch, Dennis D. (2011) 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' February 8, 2011, Seattle University Law Review, Vol. 34, No. 2, 2011

Koops, Bert-Jaap (2006) 'Should ICT Regulation be Technology-Neutral? Starting points for ICT regulation. Deconstructing prevalent policy one-liners' IT & Law series, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds., Vol. 9, 77-108, (The Hague: T.M.C. Asser Press)

Kuner Christopher, Cate H. Fred., Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey (2015) 'The data protection credibility crisis', International Data Privacy Law 2015 5:161-162.

Mak, Vanessa (2015) 'Private actors as Norm-setters through choice-of-law: the limits of regulatory competition', Tilburg Private Law Working Paper Series, No, 2/2015, SSRN

Margot Priest, (1997-1998) 'The Privatization of Regulation: Five Models of Self-regulation', 29 OTTAWA L. REV. 233, 237-38

Moses, Lyria Bennett (2007) 'Recurring dilemmas: The law's race to keep up with technological change' U. Ill. JL Tech. & Pol'y: 239

Robinson N. et. al. (2009) 'Review of EU Data Protection Directive: Summary' http://www.rand.org/pubs/technical_reports/TR710.htm

Roman, R., Najera, P., & Lopez, J. (2011) 'Securing the internet of things' IEEE Computer, 44(9), 51-58

Stuurman, Kees & Kamara, Irene (2016) 'IoT standardization. The approach in the field of data protection as a model for ensuring compliance of IoT applications?' IEEE Computer - Conference Publishing Services, pp: 336-341

Srinivasan, Raji (2008) 'Sources, characteristics and effects of emerging technologies: Research opportunities in innovation' Industrial Marketing Management 37.6, 633-640

Sweeney L. (2002) 'k-anonymity: a model for protecting privacy'. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 557-570

Tamanaha Brian (2012) 'The History and elements of the rule of law' Singapore Journal of Legal Studies, 232-247

Tsai, Janice Y., et al (2011) 'The effect of online privacy information on purchasing behaviour: An experimental study.' Information Systems Research 22.2, 254-268

Tsormpanoudi Pagona, Bettina Berendt, Fanny Coudert (2016) 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Berendt B., Engel T., Ikonomou D, Le Metayer D. and Schiffner S. (eds), *Privacy Technologies and Policy, Third Annual Privacy Forum, APF 2015, Luxembourg,* (Springer)

Van Gestel R., H.-W. Micklitz (2013) 'European Integration through standardisation: how judicial review is breaking down the club house of private standardisation bodies' Common Market Law Review 50, 145-182

Verhulst, Stefaan G. and Price, Monroe E. (2000) 'In Search of the Self: Charting the Course of Self-Regulation on the Internet in a Global Environment' Cardozo Law School, Public Law Working Paper No. 015

Weber Rolf (2010) 'Internet of Things - New Security and privacy challenges' Computer Law & Security Report 01, 26(1), p.23-30

Ziegeldorf J.H., Garcia Morchon O., Wehrle K. (2014) 'Privacy in the Internet of Things: threats and challenges' Security and Communication Networks 7.12, 2728-2742

Statutes

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No108.

Council of Europe, Recommendation (68) 509 on Human Rights and Modern Scientific and Technological Developments, adopted by the Assembly on 31st January.

Council of the European Union (2015) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), 3rd June 2015

Directive 1995/46/EC of the European Parliament and of the Council, 1995 OJ L 281 31

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

European Commission (2015) M/530 Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy

European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, 25th January 2012

European Commission (2015) Vademecum on European Standardisation in support of Union Legislation and Policies, Part I, Role of the Commission's Standardisation requests to the European Standardisation Organisations, Commission Staff Working Document, SWD 205 final

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)).

European Union, Charter of Fundamental Rights of the European Union, 7 December 2000, Official Journal of the European Communities, OJ C 364/01,18 December 2000

European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, L 119/1, 4.5.2016

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance

Treaty on the Functioning of the European Union, OJC 326, 26 October 2012, p. 47-390.

Links

http://www.phaedra-project.eu/wp-content/uploads/Findings-and-recommendations-18-Jan-2015.pdf

http://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

http://www.cencenelec.eu/standards/DefEN/Pages/default.aspx

http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/index_en.htm

---

[1] Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University the Netherlands, i.kamara@tilburguniversity.edu , Research Group on Law, Science, Technology and Society, Vrije Universiteit Brussel. This article was originally presented in the PhD Forum "Law and Governance in the Digital Era" in November 2015 in Amsterdam. The author would like to thank prof. Francesca Bignami (discussant of the article in the PhD Forum) and Matthias Pocs for their comments on an earlier version of this article. The author would also like to thank the EJLT reviewers for their feedback.

[2] Vanessa Mak (2015) characterises as *hybrid regulation* the regulation which ' *is given shape by public actors, including legislators as well as agents who have been assigned certain regulatory or enforcement powers and by private actors* '.

[3] Phaedra project deliverable (2015) http://www.phaedra-project.eu/wp-content/uploads/Findings-and-recommendations-18-Jan-2015.pdf

[4] One of such conditions is that technical standards are in line with the relevant legal provisions.

[5] ISO/IEC 27018:2014

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, L 119/1, 4.5.2016

[7] Articles 40 (Codes of conduct), 42 and 43 (certification) and several others are related to technical standards i.e. 20 (data portability), 25 (Data Protection by Design and by Default) GDPR.

[8] A definition of co-regulation could be: 'co-regulation' as systems that 'combin[e] state- and non-state regulation' and contrasting it with self-regulation, which does not entail 'any state involvement': Hans-Bredow Institut, 'Final report: Study on Co-Regulation Measures in the Media Sector', 2006

[9] There are three European Standardisation Organisations (ESOs), CEN, CENELEC and ETSI. CEN, the European Committee for Standardisation, brings together national standardisation bodies from 33 European countries.

[10] The overview provided here is not exhaustive.

[11] See http://www.cencenelec.eu/standards/DefEN/Pages/default.aspx

[12] This is a non-exhaustive overview of types of standards.

[13] http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/index_en.htm

[14] See section 2.1

[15] OJ L 55, 28/2/2011

[16] See for example European Commission guidance on how to follow-up a mandate referring explicitly to the independence of the ESOs: Follow-up of Mandates

[17] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011 - C7-0025/2012 - 2012/0011(COD)). Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), 3rd June 2015

[18] Art. 40 and 41 GDPR

[19] A 'standard means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory (..)' (art. 2 1025/2012 Regulation).

[20] There is an inconsistency in the use of terms 'privacy' and 'personal data protection' in the standardisation request. The terms are in some parts seemingly used interchangeably. However, the right to private life and the right to protection of personal data are distinct rights enshrined in art. 7 and art. 8 respectively of the Charter of Fundamental Rights of the EU. In line with this remark, 'data protection by design and by default' is different than 'privacy by design and by default', both in terms of content since they correspond to two different rights, and of legal status, since 'data protection by design and by default' is a legal obligation, established in art. 25 GDPR.

[21] Read for instance about predictive policing and surveillance societies Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. Technology-led policing, 20, 165.

[22] The author also includes "dominant design" as one of the possible characteristics, which is not as relevant to the scope of this paper.

[23] A network effect arises when "the value of the hardware and software to each user increases when other also use the product". Yoffie, David B. *Competing in the age of digital convergence*. Harvard Business Press, 1997, p.256.

[24] The aim of this section is to demonstrate potential risks of emerging technologies, not an exhaustive listing of data protection and privacy risk of any technology included under the umbrella term Internet of Things.

[25] See infographic from Intel, "A guide to the Internet of Things", no date: http://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png

[26] Information asymmetry in such cases is the gap between the controller's and the data subject's knowledge of what will happen to the latter's data. Tsai, Janice Y., et al. "The effect of online privacy information on purchasing behaviour: An experimental study." Information Systems Research 22.2 (2011): 254-268, p. 1.

[27] Reeds (2007) provides the example of example of criminal law and a murder case to illustrate the example of technology indifferent law.

[28] Technology neutral differs from technology independent: "Technology-independent regulation ought to abstract completely away from technology, whereas technology-neutral regulation might be closely related to or intertwined with technology, as long as it does not favor one specific technology over another." Koops, Bert-Jaap, "Should ICT Regulation be Technology-Neutral?"*Starting Points For Ict Regulation.Deconstructing Prevalent Policy One-Liners*, IT & Law Series, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds., Vol. 9, pp. 77-108, The Hague: T.M.C. Asser Press, 2006.

[29] European Commission proposal (2012), Recital 13

[30] Koops argues in relation to sustainability of law: "(...) Eminently sustainable laws may also contain the risk that over the years, the interpretation of the law will diverge for different technologies and hence will lead to unintended technology specificity". Koops, Bert-Jaap, Should ICT Regulation be Technology-Neutral? Starting points for ICT regulation. Deconstructing prevalent policy one-liners, IT & Law series, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds., Vol. 9, pp. 77-108, The Hague: T.M.C. Asser Press, 2006

[31] For analysis of the concepts of privacy by design, data protection by design and by default read: ENISA, Privacy and Data Protection by Design, 12 January 2015, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design ; Ann Cavoukian, Privacy by Design, Seven Founding Principles, https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

[32] Art. 25(1) GDPR

[33] There is already standardisation activity in ISO and IEC, in the field of data portability and interoperability in information security and cloud computing (ISO/IEC DIS 19941)

[34] The mandate is based on the Commission proposal for GDPR of 2012. The numbering of articles in the Commission proposal is different from the final text of the 679/2016 GDPR, which was adopted later.

[35] Currently, the work of the JWG8 is ongoing and is too early for any substantial commentary on the (unpublished) work of the JWG8.

[36] '*i) How to address and manage privacy and personal data protection issues during the design and development and the production and service provision processes of security technologies and services, allowing manufacturers and service providers to develop, implement and execute a widely recognised Privacy by Design (PbD) approach in their processes; and ii) European standards addressed to the manufacturers and service providers when specifying the privacy and personal data protection management processes with an explanation how to realise them, including descriptions of the necessary roles, tasks, documentation, hardware and software requirements, and templates to be used when applying the requested standard(s).*'

[37] Art. 4(9) GDPR

[38] The paradox is that the fulfilment of the legal obligation (data protection by design and by default) by the person responsible (data controller/customer of security products/systems) is heavily dependent on persons (manufacturers of security products/systems who design the products/systems) not subject to the data protection legislation.

[39] See M/530 (p.7): '*Whilst legally speaking the customers of the security industry often bear the legal responsibility for complying with data protection rules (being the data controllers), their providers also bear some responsibility for data protection from a societal and ethical point of view.* '

[40] M/530 p. 10

[41] This analysis is not in the scope of this article.