Claudia Quelle

Privacy, Proceduralism and Self-Regulation in Data Protection Law

1. Introduction

Contemporary data flows and uses of data have made it yet more pertinent than before to regulate both market and government entities. On both fronts, data protection law places strong reliance on procedures, shying away from substantive limitations. Many share the concern of Bennet that data protection law cannot «control the voracious and inherent appetite of modern organizations for more and more increasingly refined personal information»[1]. This article, too, places a critical note regarding the ability of EU data protection law to substantially limit the collection and use of personal data in the private sector, problematizing the role of corporations in the regulatory framework. The General Data Protection Regulation relies on a degree of self-regulation, particularly on the side of corporate actors involved in the processing of personal data. The very actors which were seen to encroach upon the private sphere, are given an increasingly important role in setting the boundary between what is and what is not acceptable.

First, this article sketches the circumstances under which data protection law came to regulate both the public and the private sector, it is still pertinent today that we have an "omnibus regime"[2]. The second part of this article argues that data protection is to a large extent about *the way in which* the boundary between lawful and unlawful processing operations is drawn, and in particular, about who gets to have a say. The "processing" of personal data encompasses any operation performed on personal data, including collection, use, dissemination, and storage[3]. How does data protection law determine whether or not personal data can be processed? And how does this relate to privacy? The third part of this article describes the distribution of decisional competence between three central actors: individuals, controllers (the entities processing the data), and supervisory authorities. Control or participation on the part of the individual has long been emphasized, but this tenet appears to be losing force. Finally, this article problematizes the re-distribution of competence towards controllers themselves from a regulatory perspective.

1 C. J Bennett, *In Defence of Privacy: The Concept and the Regime*, in «Surveillance & Society», vol. 8, 2011, p. 494.

2 Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, p. 16.

3 GDPR, art. 4(2).

This article will focus on the General Data Protection Regulation (GDPR), which will officially replace the current Data Protection Directive from 25 May 2018 onward. It applies to both public and private entities, but excludes data processing in the areas of criminal law enforcement and of national security[4]. The EU has adopted separate instruments concerning the processing of data by Community bodies, data protection in the area of criminal law enforcement, and for the electronic communications sector.

2. One Data Protection Law to Rule Them All

Data protection law is in a peculiar bind. In short, it aims to protect individuals against abuses of power on the side of the government as well as on the side of privately held corporations. It is a relatively new field of law, arising in the 60s and 70s to tackle «the problem of privacy and computers»[5]. Data protection laws began to surface after computers made their appearance in daily administration. On the one hand, the shift of responsibility from the individual citizen to society at large required — in the words of Mayer-Schönberger — «a sophisticated system of government planning, and planning requires data»[6]. Bennett explains that the provision of the social services which we have come to expect, requires the collection of large amounts of information about individuals.[7] EU resolutions at the time show that the EU was eager to foster a data processing industry[8]. At the same time, however, the increasing automation in the public sector, as well as the increase in computing power, had given rise to civil unrest. It was feared that the «automated and largely dehumanized bureaucracy» would affect the balance of powers, strengthening public administration and the executive[9]. The speed of technological developments already set back the legislature, as it had to rely on studies and reports to be able to make adequate laws.

Databanks were quickly established also by private parties, both to aid their administration and «as an aim in itself, to provide information as a public service or as a negotiable commodity»[10]. According to Hondius, legislative action targeting private parties was particularly spurred by the latter development. Over 40 years later the business of data brokers is a force to be reckoned with. Data is collected through cookies

4 GDPR, art. 2(2)(d).

5 F. W. Hondius, *Emerging Data Protection in Europe*, North Holland Publishing Company, Amsterdam, 1975, p. 7.

6 V. Mayer-Schönberger, *Generational Development of Data Protection in Europe*, in P. E. Agre, M. Rotenberg (eds.), *Technology and Privacy: The New Landscape,* MIT Press, Cambridge, Massachusetts 1997, p. 219 and p. 222.

7 C. J. Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaza, 1992, p. 19.

8 See e.g. Resolution embodying the Opinion of the European Parliament on the Communication from the Commission of the European Communities to the Council containing initial proposals for priority projects in data-processing, O.J. No C239 of 20.10.1975.

9 F. W. Hondius, *Emerging Data Protection in Europe*, cit., p. 5.

10 *Ivi*, p. 10.

and other means, to be analysed and sold by data brokers. The data is used for a variety of purposes, not only to serve behavioural advertising, but also for the prevention of credit card or tax fraud, credit scoring, law enforcement, and research. Traditional data sources are insufficient to score "thin file" borrowers, so a number of start-ups in the U.S. credit scoring industry have started to collect a wide variety of data under an "all data is credit data" approach. This includes not only purchase and payment history but also, for example, geographical location and networks (friends) on social media[11]. The Dutch tax authority is on the look-out for relevant correlations to make the tax collection system more efficient. One relatively innocent example: it sends a letter to people going through a divorce reminding them to be careful with their tax reports, because they are more prone to make mistakes[12].

Against the background of a strengthened executive and a newfound market in personal data, data protection laws were brought on, in the words of Hondius, by an «increased dissatisfaction with the type of society commanded by technocracy and mass consumption»[13]. Similar concerns are still at play in the field of data protection today. Data processing technologies continue to improve the ability of government researches to carry out their tasks, e.g. through fraud prevention schemes. A recent example from the Dutch context is the use of Automatic Number Plate Recognition (ANPR) data for tax purposes. The national police force obtains data through cameras on the main roads; the pictures are analysed using ANPR software. The Dutch tax authority has been making use of this police database, e.g. to check whether company cars were used for unregistered private purposes, despite the absence of a legal ground to legitimate this processing activity[14]. The private sector also plays an important role in the contemporary data processing landscape. Not only can data collected by private firms be accessed by government entities for their own purposes; a number of corporations are increasingly influential in both public and private spheres, as they create and manage platforms for communication, e-commerce and entertainment. Private firms use personal data for behavioural advertising, the personalisation of search results and news feeds, to make recommendations, and, more generally, to improve pricing and risk management models so as to maximize the ability to extract surplus from consumers[15].

Data protection law is still accompanied by both a weariness of government authority and of the power of corporate actors. Cohen argues that the purpose of these private and private-public data flows is to «produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories (…) stimuli are tailored to play to existing inclinations, nudging

11 M. Hurley, J. Adebayo, *Credit Scoring in the Era of Big Data*, in «The Yale Journal of Law & Technology», vol. 18, 2016, pp. 148-216.

12 M. Martijn, *Baas Belastingdienst over Big Data: Mijn Missie Is Gedragsverandering*, in «de Correspondent», 2015 [accessed 7 April 2017].

13 F. W. Hondius, *Emerging Data Protection in Europe*, cit., p. 7.

14 Hoge Raad, 24 January 2017, ECLI:NL:HR:2017:288.

15 J. E. Cohen, *What Privacy Is For*, in «Harvard Law Review», vol. 126, 2013, p. 1916.

them in directions that align with profit-maximizing goals»[16]. She draws from theories of decentralized forms of surveillance, under which surveillance is not (only) visibly exercised by a number of central institutions at particular moments in time. It is instead tied to the continuous "modulation" by private actors in the market[17], and results from the convergence of different systems of control ("surveillant assemblages")[18]. It is not at all clear that "dataveillance"[19] occurs solely for the one purpose of creating predictable and profit-generating consumers[20], but Cohen's point is well-taken. A related but distinguishable phenomenon in the area of dataveillance is the use of data for social sorting and access controls, potentially through fully or largely automated processes[21]. Kerr and Earle have introduced the concept of preemptive predictions to refer to the situation in which «predictions are intentionally used to diminish a person's range of future options», such as the use of no-fly lists which ban potential terrorists or the use of profiles to sort through job applicants[22]. Again, both the public and the private sector make use of "big data" to change our lives.

3. Drawing the Boundary between the State, the Private, and the Market

Privacy and data protection have a complex relationship[23]. In the context of the processing of personal data, data protection law protects a number of special interests, only some of which fall squarely within the meaning of *privacy*. We can list, for example, the interest to have some things remain unknown; the interest not to have data profiles used to manipulate and control you; and the interest in fair and equal treatment by artificial intelligence[24]. Engaged in the comparison, one inevitably runs into the problem that it is unclear what *privacy* entails. In this article, I see privacy as pertaining to *the private* as opposed to *the public*, whereby the public is understood as encompassing both state involvement and intrusions

16 *Ivi*, p. 1917.

17 See G. Deleuze, *Postscript on the Societies of Control*, in «October», vol. 59, 1992, pp. 3-7.

18 See K. D. Haggerty, R. V. Ericson, *The Surveillant Assemblage*, in «British Journal of Sociology», vol. 51, 2000, pp. 605-622.

19 R. A. CLarke, *Information technology and dataveillance*, in «Communications of the ACM» vol. 31, 1988.

20 Bennett and Raab have summarized a number of different causes of surveillance, including "Weberian bureaucratic rationality", "the deterministic logic or technological application", and "the demands of the capitalist mode of production". (C. J. Bennett, C. D. Raab, *The Governance of Privacy*, The MIT Pres, Cambridge, Massachusetts, 2006, p. 19).

21 M. Galic, T. Timan, B.-J. Koops, *Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation*, in «Philosophy & Technology», vol. 30, 2017, pp. 28-29.

22 I. Kerr, J. Earle, *Prediction, Preemption, Presumtion: How Big Data Threatens Big Picture Privacy*, in «Stanford Law Review Online», vol. 66, 2013, pp. 67-68.

23 See e.g. G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Cham, 2014; S. Gutwirth, R. Gellert, *The Legal Construction of Privacy and Data Protection*, in «Computer Law & Security Review», vol. 29, 2013, pp. 522-530.

24 GDPR, recital 71.

from the market. Data protection law regulates the processing of personal data to ensure that it is just, e.g. that it does not discriminate, but it also protects the privacy of individuals. This is because data protection law regulates how the boundary between the public and the private is drawn. Thus, it does not conclusively strike «the balance between privacy and community values»[25], but rather determines the way in which this "balance" is struck, according differing degrees of decisional competence to a range of actors.

3.1 Procedural Legal Norms to Regulate What is, or is not, Private

When data protection law applies, it determines whether, and for what purposes, personal data can or cannot be processed. Burkert's division of data protection law into "material" and "procedural" rules still largely holds true. Material norms guard against «the "natural" tendencies of the medium (electronic-processing)»[26]. Under the Data Protection Directive, as well as under the new GDPR, data must be processed lawfully, fairly, and in a transparent manner; it must be collected for specified, explicit and legitimate purposes and processed and stored only insofar as is adequate, relevant and necessary to achieve the purposes; and it must be kept accurate and up to date. These norms are frequently referred to as the "data quality principles". The GDPR adds two other obligations to the list, elevating them to the status of a "principle": that personal data must be processed in a manner which ensures an appropriate level of security and that the controller is responsible for, and able to demonstrate compliance with, the other principles[27]. The data quality principles are rarely used to address the question for which purposes personal data can be processed, let alone the question whether this purpose is worth the risks posed by the processing operation[28]. According to Burkert, they are neutral, in the sense that they could equally apply to the processing of personal data by «criminal organisations»[29] or, indeed, by authoritarian regimes. While they could use the fairness principle or the requirement that the purpose must be legitimate to engage in a substantive assessment, supervisory authorities tend to steer away from such political intervention. They focus, instead, on the question whether there is a legal ground for the processing.

The requirement to have a legal ground for the processing refers to a number of procedures to limit, as well as legitimize, the type of processing operations which are permissible. As explained by Bennett and Raab, data protection law is founded on the assumption that «privacy is a highly subjective value», so that «the content of privacy rights and interests have to be defined by individuals themselves

25 C.J. Bennet, C.D. Raab, *The Governance of Privacy*, cit., p. 6.

26 H. Burkert, *Data-Protection Legislation and the Modernization of Public Administration*, in «International Review of Administrative Sciences», vol. 62, 1996, p. 558.

27 DPD, art 6; GDPR, art 5.

28 Article 29 Data Protection Working Party, "Opinion 03/2013 on Purpose Limitation", 2013, pp. 19-20.

29 H. Burkert, *Data-Protection Legislation and the Modernization of Public Administration*, cit., p. 559.

according to context»[30]. The legal grounds in the Data Protection Directive and the GDPR are: the informed consent of the data subject; the performance of a contract to which the data subject is party; compliance with a legal obligation; the protection of the vital interests of an individual; the performance of task of public interest or of official authority; and the legitimate interest of the controller[31]. In practice, this means that the processing of personal data is frequently legitimized because of a bilateral arrangement with the individual concerned (consent and contract), or because it was deemed acceptable through collective, democratic decision-making procedures (compliance with a legal obligation, performance of official authority)[32]. The procedures of consent, as well as the prior check and the data protection impact assessment, will receive more attention in section 4.

When faced with the question whether a particular type of dataveillance is too intrusive, data protection law turns to its procedural norms[33]. This is why data protection law can be understood as attributing and distributing decisional competence with respect to the question whether, and for what purposes, personal data can be collected, shared and used[34]. It thereby accords individuals as well as other actors a say over the boundary between what is public (e.g. pertaining to the exercise of public administration), and what is private (e.g. not the state's business).

3.2 The Grey Zone between the Private and the Public

Data protection law regulates the public-private boundary by regulating the grey zone between what is clearly private and what is clearly public. Data protection law, itself a public intervention, does not cover purely private activities. It contains an exemption for the processing of data by an individual «in the course of a purely personal or household activity» (the "household exemption")[35]. Previous versions of the law referred to the "domestic"[36], and to the "right to privacy[37]. The reference to the household signals a clear link with the inviolability of the home, which is, notes Gonzalez-Fuster, a precursor of modern privacy rights[38]. Thus, data protection law does not intrude into the private sphere.

30 C. J. Bennett, C. D. Raab, *The Governance of Privacy*, cit., pp. 8-9.

31 GDPR, art 6(1).

32 H. Burkert, *Data-Protection Legislation and the Modernization of Public Administration*, cit., pp. 559-560.

33 K. D. Haggerty, *What's Wrong with Privacy Protections?* in A. Sarat (ed.), *A World Without Privacy*, Cambridge University Press, Cambridge 2014, p. 210.

34 L. A. Bygrave, D. W. Schartum, *Consent, Proportionality and Collective Power*, in Y. Poullet, S. Gutwirth, P. De Hert, C. de Terwangne, S. Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht 2009, pp. 157-73 and pp. 157-58.

35 GDPR, art 2(2)(c).

36 DPD, recital 12.

37 G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, cit., p. 126.

38 *Ivi*, p. 24.

Data protection law also does not regulate things which cannot be tied to specific individuals. The GDPR applies to the processing of *personal data*: data which can be linked to an identifiable or identified individual or which is used to impact the rights and interests of same identifiable person in particular, i.e. someone who is "singled out"[39]. The concept of personal data also covers information which would not be considered as "private", although it could potentially be analysed and used in ways which encroach upon the private sphere of an individual. The fact that data protection law does not limit itself to "private data", extends the say of individuals regarding what should be considered as private, given the circumstances at hand. Bennett and Raab use the example of telephone directories: many people do not unlist their phone number, but celebrities, battered wives, and police officers might choose differently[40].

The fact that data protection law does not give individuals a say with regard to *all* data processing operations, is to limit their decisional competence to things which directly or especially influence them individually in ways they might consider to be invasive or unjust. Affairs which are not especially linked to individuals, but which rather pertain to society as a whole, should arguably not be subject to individual control mechanisms. In that case, the "collective" decision-making process of parliamentary democracy is often a more appropriate route. It is also possible to consider involving groups of stakeholders — e.g. during the data protection impact assessment —, as they are together affected by the profiles within which they are placed[41].

3.3 The Market as Part of the Public

As argued in section 2, privacy concerns also arise when data is processed by corporate entities. It is therefore appropriate that the GDPR gives individuals the same rights and protections in the private sector, particularly vis-à-vis corporations as well as individuals engaged in commercial activity or offering professional services. Data protection law thus regulates not only the boundary between the private and the state, but also between the private and the market. Individuals can object to the commodification of their personal data and to corporate forms of dataveillance. Such private sector activity falls within the grey zone between the public and the private, discussed above.

Early data protection laws were drafted with a view to abuse and misuse of data by government entities and large organisations. Nowadays, however, data protection law has to grapple with the fact that individuals also widely make use of ICT technologies[42]. As a result of the household exemption, such activity is partly unregulated. The household exemption does not apply when personal data is pro-

39 Article 29 Data Protection Working Party, "Opinion 4/2007 on the Concept of Personal Data", 2007, pp. 10, 14.

40 C. J. Bennett, C. D. Raab, *The Governance of Privacy*, cit., p. 9.

41 A. Mantelero, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in L. Taylor, L. Floridi, B. van der Sloot (eds.), *Group Privacy*, Springer, Dordrecht 2017, pp. 139-58.

42 B. Van Alsenoy, *The Evolving Role of the Individual under EU Data Protection Law*, in «ICRI Working Paper Series», 2015, pp. 1-36.

cessed in relation to «a professional or commercial activity»[43] indicating that other levels of activities law outside the scope of the GDPR. This might be a break with earlier case law and policy, under which the activities of private individuals more readily fell within the scope of data protection law[44]. The GDPR, however, appears to be based on the assumption that individuals only need to be protected from other private entities when they might suffer from the types of power imbalance which we can find on the market.

4. The Allocation and Distribution of Decisional Competence

In regulating how the boundary between the private and the public is drawn, data protection law accords decisional competence to a number of actors, amongst whom the following three exercise it most regularly: **controllers** (the entities which process the data), **data subjects** (the individuals whose data is being processed), and **supervisory authorities** (the institutions tasked with oversight, enforcement, complaints handling, the provision of guidance and the approval of codes of conduct, etc.)[45]. Other important actors include the legislature, data protection officers, the European Data Protection Board, certification bodies and standard-setting organisations.

Data protection law has always involved the three actors mentioned above, but the configurations of the distribution of their competence have changed over time. If a general trend can be discerned, it might be from (1) the supervisory authorities as *ex ante* privacy protectors, through licensing schemes are the prior checking system, to (2) the data subjects, through the consent procedure and their rights of control, to (3) the controllers and their responsibility to process data in accordance with the risks posed by processing operations to the rights and freedoms of individuals[46].

The role of data subjects is most emblematic of data protection law and will be discussed first. The remainder of this article describes a shift away from individual control. This shift is taking place through amendments to a particular procedure: the prior check.

4.1 The Involvement of Individuals

A significant feature of contemporary data protection law is that individuals are awarded a certain "control" within the framework of state authority. When data is

43 GDPR, recital 18.

44 See e.g. Article 29 Data Protection Working Party, "Statement of the Working Party on Current Discussions Regarding the Data Protection Re-Form Package, Annex 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities", 2013.

45 L. A. Bygrave, D. W. Schartum, *Consent, Proportionality and Collective Power*, cit., p. 158.

46 Cfr., V. Mayer-Schönberger, *Generational Development of Data Protection in Europe*, cit.; M. E. Gonçalves, *The EU data protection reform and the challenges of big data: remaining uncenrtainties and ways forward*, in «Information & Communications Technology Law», vol. 26, 2017, p. 104.

obtained or used without the knowledge of the individual, she is rendered visible or transparent to whoever accesses the data, and is thereby precluded from the ability to "withdraw from society"[47]. According to Mayer-Schönberger, the involvement of individuals evolved from "all-or-nothing" rights to (refuse to) consent to a processing operation – giving individuals the option, in theory, to "ward off society in personal matters" – to a refined set of rights which grant individuals participatory rights with respect to every phase of the data processing operation[48]. In keeping with the German tradition of informational self-determination, he considers a participatory framework as the third generation of data protection[49]. It is, however, still common to see the control rights as a protection of "the right to be let alone"[50].

Thus, the GDPR determines whether data subjects can withdraw themselves from the reach of the public, for example by objecting to the use of ANPR databases to enforce tax law. Or, from a different perspective, it gives data subjects rights which might help shape how power is exercised in society, at least vis-à-vis their own person. Either way, data protection law permits them to have "a measure of influence"[51] over whether or how their data is used, and thus over whether or how "the public" can impact their lives.

European data protection law has long included a number of rights without, however, explicitly granting individuals a say. The right of access and other transparency measures can limit chilling effects, whilst the right to rectification can prevent inaccurate judgment. These rights offer «a means for a data subject to oversee and enforce observance of the law» which «would be devoid of logie if those who hold other people's persona! data were not subject to any rules»[52]. It is only quite recently that the question whether the processing operation was necessary for some legitimate purpose to start with, can be answered by individual data subjects. The most well-known first-generation data protection act, the 1970 *Datenschutz* of the German land of Hesse, granted two distinct powers to individuals: the right to rectify incorrect data, and the power of individuals whose rights had been infringed by *unlawful* access, alteration or destruction or by *unlawful* extraction, to require that such actions are discontinued[53]. The federal *Bundesdatenschutzgesetz* of 1977 explicitly placed the rights of data subjects in a larger framework concerned with the misuse of data, all with the purpose of safeguarding the "legitimate inte-

47 The International Commission of Jurists, *The Protection of Privacy*, in «International Social Science Journal», vol. 24, 1972, pp. 423-428.

48 V. Mayer-Schönberger, *Generational Development of Data Protection in Europe*, cit., pp. 226, 229-230.

49 P. M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, in «Iowa Law Review», vol. 80, 1995, pp. 553-564.

50 S. D. Warren, L. D. Brandeis, *The Right to Privacy. The Implicit Made Explicit*, in «Harvard Law Review», vol. 4, 1890, pp. 193-220. See also C. J. Bennett, C. D. Raab, *The Governance of Privacy*, cit., p. 6.

51 L. A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014, p.158.

52 Opinion of G Ruiz-Jarabo Colomer in Case C-553107, *Rijkeboer* [2009] ECR 1-03889, paras. 33-34.

53 Hessisches Datenschutzgesetz (1970), section 4.

rests" of the persons concerned. The overall focus was on the protection of the integrity and confidentiality of records by the data protection commissioner[54]. Only later did data protection law shift from offering protection against misuse, to empowering individuals to have a say about what counts as (proper) use or misuse to start with[55].

The notion of privacy-as-control was particularly influential in early US explorations of data protection regulation. The advent of computerized data processing gave rise to the notion of "informational privacy", referring to be ability of individuals to control the data which refers to them, and in particular when, how and to what extent the data is communicated to others[56]. A first report on the "Fair Information Principles" emphasized the responsiveness of the record-keeper and the ability of individuals to hold record-keepers to account, so as to reduce the power which accrues to them. The report writes:

> «Today it is much easier for computer-based record keeping to affect people than for people to affect computer-based record-keeping (…) There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers – unknown, unseen and, all too frequently, unresponsive»[57].

Under contemporary EU data protection law, controllers are required to be, to some extent, responsive to the wishes of data subjects. Few provisions in contemporary data protection accord to the individual a greater say over the boundary between permissible and impermissible data processing operations, than the right to object. While the legal ground of consent enables the data subject to permit data processing operations which would otherwise be unlawful, the right to object empowers her to preserve or expand her private sphere. This right, included in the Data Protection Directive and in the GDPR, gives data subjects the power to contest whether the processing of data is legitimate and proportionate. It is available when the data processing operation was, in first instance, legitimised by its necessity for the execution of a task carried out in the public interest or the exercise of official authority, or by the legitimate interest of the controller. If this right has been exercised, it is up to the controller to show compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. There are special arrangements for these types of cases: Concerning direct market-

54 BDSG (1977), sections 1(1), 4 and 7-15; C. J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United states*, cit., p. 183.184.

55 V. Mayer-Schönberger, *Generational Development of Data Protection in Europe*, cit., p. 230; L. A. Bygrave, D. W. Schartum, *Consent, Proportionality and Collective Power*, cit., p. 159..

56 See e.g. A. Westin, *Privacy and Freedom*, Atheneum, New York 1967, p. 7; C. Fried, *Privacy*, in «The Yale Law Journal», vol. 77, 1968, pp. 475-493.

57 The Secretary's Advisory Committee on Automated Personal Data Systems, "Records, Computers and the Rights of Citizens", US Department of Health, Education and Welfare, 1973, pp. 28-31.

ing, research, and automated decisions. Generally, however, the right to object does not give individuals the final say. Controllers can bring forward counter-arguments, and in case of conflicting views on "the right balance", data subjects will have to referto the supervisory authority or the court[58]. In the words of Gonzalez Fuster and Gutwirth, «the legal significance of the choices of individuai data subjects 'will afterwards, in any case, shift (back) to the hands of courts and judges»[59]. This means, *contra* Boehme-Nessler, that we cannot maintain that «the final authority on decisions about what happens with the data must lie with those affected»[60].

This procedural aspect of data protection law can be tied to the meaning of *the legal right to* privacy. How can law, which is public in nature, protect the private? It can define some things which are out of reach, but we are bound to disagree. A solitary Hohfeldian claim or duty of others to leave you alone, or, indeed, to allow you to participate in society, may not account for that which *you* consider to be private. Therefore, data protection law includes Hohfeldian powers: the legal powers of an individual or group of individuals to demand solitude or not, depending on their own choice. Following this approach, the right to privacy is not only about legal protection of the — publicly formulated — boundary between the public and the private. It is also about the way in which this boundary is set, including the power to object to overly invasive or arbitrary boundary-setting by the State and other powerful entities[61].

4.2 Licensing Schemes: Granting First Say to the Supervisory Authority

European data protection law empowers supervisory authorities to carry out *ex ante* oversight on controllers. This builds on a number of "first generation" data protection laws, which placed great reliance on so-called licensing schemes. Controllers were required to register their processing operations and to obtain a license, containing specific conditions, from the supervisory authority. The Swedish *Datalag* from 1973 required any machine-readable personal data register to be subject to the prior approval of a Data Inspection Board. Unlike the German laws of the time, the *Datalag* contained few material rules, relying on the Data Inspection Board to come up with safeguards appropriate to the context at hand[62]. The first Dutch data protection bill contained a similar regime, but with a self-regulatory twist: controllers had to propose case-specific guidelines on how to balance the interests at stake. This proposal was criticised for the lack of material rules to guide controllers, as well as for the creation of one "big

58 J. Ausloos, *The Interaction between the Rights to Object and to Erasure in the GDPR*, in «CiTiP Blog», 2016.

59 G. González Fuster, G. Gutwirth, *The Legal Significance of Individual Choices About Privacy and Data Protection*, in M. Friedewald, J. P. Burgess, J. Čas, R. Bellanova, W. Peissl (eds), *Surveillance, Privacy and Security: Citizens' Perspectives*, Routledge, London, 2017, p. 188.

60 V. Boehme-Nessler, *Privacy: a matter of democracy. Why democracy needs privacy and data protection*, in «lnternational Data Privacy Law», vol. 6, 2016, p. 224.

61 Cfr., G. González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, cit., p. 23.

62 *Ivi*, p. 59.

brother" to watch over privacy. As a result, the data quality principles were included in the bill, and the *ex ante* check was abolished[63]. Like the Hessian and federal German data protection acts, the resulting *Wet persoonsregistraties* did not contain a licensing scheme. The French *loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 found a middle ground*. This data protection act contained relatively detailed rules on the permissibility of data processing. Against this backdrop, it required some processing operations to be notified to the supervisory authority, whereas for others, the availability of a legal ground was sufficient[64].

Bygrave and Wiese Schartum argue that licensing schemes were abandoned due to their paternalistic nature, in favour of mechanisms which rely on individuals to define their own interests and to decide for themselves[65]. But they were not abandoned. The national data protection acts which did not contain a licensing scheme had to be amended after the Data Protection Directive of 1995 entered into force.

The Directive introduced a limited "prior checking" system akin to that in the *loi relative à l'informatique, aux fichiers et aux libertés*. Member States had to define those processing operations which "likely present specific risks to the rights and freedoms of data subjects". Following a general notification procedure, these risky processing operations have to be examined by the supervisory authority *ex ante*[66]. Depending on the exact implementation, the prior check is either akin to a licensing scheme, granting authorities the power to draw up substantive norms to safeguard the privacy of data subjects, orto a "thick" registration, followed by a preventative compliance check against the material norms of data protection[67]. According to the Directive, the supervisory authority only has the power to either issue an opinion as to whether the processing would be incompliant, or authorize the processing operation[68]. Most Member States, however, also granted their authorities the power to reject processing operations which are likely to present specific risks[69]. In practice, a number of authorities find that the procedure helps them to control large processing operations[70]. Even in its thinnest form, the prior checking procedure accords a hefty decisional competence to supervisory authorities. They are empowered to opine on a processing operation before it is started

63 M. Overkleeft-Verburg, *De Wet Persoonsregistraties. Norm, Toepassing En Evaluatie*, Katholieke Universiteit Brabant, Tilburg 1995, pp. 84-98.

64 G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, cit., pp. 64-65.

65 L. A. Bygrave, *Data Privacy Law: An International Perspective*, cit., p. 159.

66 DPD, arts. 18 and 20(1).

67 See on the difference between a licensing model and a registration model: C.J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, cit., pp. 158-60.

68 DPD, recital 54.

69 Commission, "Impact Assessment Accompanying the General Data Protection Regulation", 2012, Annex 1, 3.12.3.

70 G. Le Grand and E. Barrau, *Prior Checking, a Forerunner to Privacy Impact Assessments*, in D. Wright, Paul De Hert (eds.), *Privacy Impact Assessment,* Springer, Dordrecht, 2012, p. 97, p. 111.

– before data subjects have had the chance to be involved. Indeed, the licensing model implicitly rejects data protection models based on data subject control[71].

4.3 The Data Protection Impact Assessment: Granting First Say to the Controller

4.3.1 Accountability and Discretion

As norm-addressees, controllers are tasked with the application of the law. In first instance, it is up to them to decide, for example, whether the purpose of their processing operations is too wide to count as "specified". Under the GDPR, this role of controllers is supported with the aim to enhance compliance[72]. Article 5 now includes the principle of accountability, which is fleshed out in Article 24, concerning the responsibility of the controller:

> «Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation».

The GDPR puts in place a number of "meta-regulatory" obligations to regulate how the controller is to apply data protection law. This includes the requirement to keep records, to appoint a data protection officer, and to carry out the data protection impact assessment of Article 35. Many of these duties only apply when the processing operation poses a high risk to the rights and freedoms of individuals.

The notion of "risk" also guides controllers in their application of the material and procedural norms in the GDPR. It follows from Article 24 that the implementation measures taken by controllers should in fact be suitable to protect the rights and freedoms of individuals. In other words, the notion of a risk to the rights and freedoms of individuals short-circuits the GDPR from the bottom (implementation) to the top (the goal to protect the rights and freedoms of individuals). This means, concretely, that the question whether the processing is fair or whether the purpose is legitimate, is opened up[73].

The compliance measures should not only be suitable to protect the rights and freedoms of individuals; the envisaged processing operation also has to be proportionate, given the purpose for which it is to be conducted. Controllers are required

71 C. J. Bennett, *Regulating Privacy: Data Protection and Public Poticy in Europe and the United States*, cit., p. 162.

72 Article 29 Data Protection Working Party, "Opinion 3/2010 on the Principle of Accountability".

73 C. Quelle, *The Risk Revolution in EU Data Protection Law: We Can t Have Our Cake and Eat It, Too*, in R. Leenes, R. van Brakel, S. Gutwirth, P De Hert (eds), *Data Protection and Privacy: The Age of Intelligent Machines*, Hart Publishing, 2017, pp. 11-12.

to assess the proportionality of their processing operation, as well as the risks to the rights and freedoms of individuals, as part of the data protection impact assessment of Article 35. This is a significant redistribution of decisional competence. Proportionality has to be assessed irrespective of the legal ground which the controller intends to rely on, with one exception: the case in which there is a legal basis for the processing, for which a regulatory impact assessment has been carried out[74]. Thus, while they are not reality asked to do over the assessment made by parliament, their judgment does pre-empt that of individuals. Controllers have to assess whether the processing operation is proportionate before data subjects have had the chance to decide whether or not they would give their consent.

It is important to emphasize that by enabling controllers to apply the law "properly", this accountability - and risk-based approach also confers a certain discretion on them. It enlarges their decisional competence. While Gonçalves refers to a «decisive power»[75], controllers do not have full discretion to decide what counts as a risk and whether the processing operation is too risky. To start, the GDPR contains a number of factors in light of which the notion of a risk to the rights and freedoms of individuals is applied, including the nature, scope, context and purposes of the processing (also mentioned in Article 24)[76]. The application of the law will continue to take place within the legal framework provided by the legislature, as interpreted by the courts. As discussed below, supervisory authorities, individuals, and associations of controllers are also accorded a role.

4.3.2 Guidance Documents and the Prior Consultation

Supervisory authorities can regulate how controllers assess "risk". They have already been devising risk assessment methodologies, such as the Informational Commissioner's Office "Privacy Impact Assessment Code of Practice". The GDPR explicitly empowers them to draw up lists regarding the type of processing operations which do, or do not, pose high risks to the rights and freedoms of individuals[77].

So far, the Article 29 Data Protection Working Party has not been too keen on providing detailed guidance. lt has drawn up a list of generai criteria which methodologies should adhere to, relying explicitly on controllers themselves, codes of conduct, and on sector-specific frameworks which draw on «specific sectorial knowledge»[78]. The decisional competence which was awarded to the authorities under the prior checking system, is retained, at least in part. Following Article 36, the controller has to consult the authority if the impact assessment indicates «that

74 GDPR, art. 35(10); Article 29 Data Protection Writing Policy, Guidelines on Data protection Impact Assessment (DPIA), WP 298, 4 October 2017, p. 13.

75 M. E. Gonçalves, T*he EU data protection reform and the challenges of big data: remaining uncertainties and ways forward*, cit. p. 104.

76 GDPR, recital 76.

77 GDPR, arts. 35(4) and (5).

78 The Article 29 Data Protection Workin Party, *Guidelines on Data Protection Impact Assessment (OPIA)*, cit., p. 17.

the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk». The prior consultation of Article 36 does envisage a smaller role for the supervisory authority than the prior checking system. To start, it is not backed up by a notification duty, as was the prior check of the Data Protection Directive[79]. Only if controllers decide to start the procedure, do they have to submit the report of the data protection impact assessment[80]. The controllers will have to determine themselves whether it is appropriate to consult with the supervisory authority before starting their processing operation, i.e. whether the processing would result in a high risk. Secondly, the prior consultation may not have to be carried out for each risky processing operation. The GDPR is ambiguous as to whether the controller still has to check with the supervisory authority if it plans on taking measures to substantially lower the level of risk[81]. According to the Article 29 Working Party, this is not necessary: a prior consultation is only required ifthe residuai risk is high[82]. This affords controllers significantly more leeway in deciding whether it is appropriate to consult with the authority: not only is it for them to decide whether the processing operation poses a high risk to start with, they also need to decide whether the mitigating measures sufficiently reduce the risk level.

If a prior consultation has been started, the supervisory authority not only has the power to give an opinion on the permissibility of the processing operation – it can also decide to ban or limit the processing, if it «is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk»[83]. As under the Directive, it is unclear whether the supervisory authority can go beyond a simple compliance check.

4.3.3 The Consultation of Stakeholders

When a data protection impact assessment is required, the controller must «seek the views of data subjects or their representatives on the intended processing». This duty only applies «where appropriate» and «without prejudice to the protection of commercial or public interests or the security of processing operations»[84]. Nonetheless, it is noteworthy that the risk-based approach formulates this new framework for participation of data subjects. On the one hand, this approach de-emphasizes the role of consent and of an individual's data subject rights. Controllers are given greater responsibility to ensure that data processing operations are legitimate. The emphasis is

79 This change was not supported by the EDPS, see the European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission - a Comprehensive Approach on Personal Data Protection in the European Union", 2011, pp. 14-15.

80 GDPR, art. 36(3)(e).

81 GDPR, recital 84, art. 36(1).

82 The Article 29 Data Protection Workin Party, *Guidelines on Data Protection Impact Assessment (OPIA)*, cit., p. 18.

83 GDPR, arts. 36(2) and 58(2)(f).

84 GDPR, art. 36(9).

again on the processing itself and its function in society. While the purpose, previously, was to prevent "misuse", now the benchmark is protection of "the rights and freedoms of individuals" (plural). This development followed years of critique on the "notice-and-consent" model, which arguably does not enable individuals to make a real and informed choice in practice[85]. Now, within the framework of the data protection impact assessment, data subjects who are likely to be impacted by the processing operation can be consulted in a different kind of setting. The framework allows, for example, for stakeholder meetings and the appointment of representatives.

4.3.4 Codes of Conduct

Finally, controllers also have a joint role in operationalising their accountability obligations by drawing up codes of conduct. Following Article 40, associations of (representatives of) controllers should be encouraged to draw up codes of conduct. A draft code must be submitted to the competent supervisory authority, which shall approve it «if it finds that it provides sufficient appropriate safeguards»[86]. Approved codes of conduct are very useful to controllers, and particularly to smaller companies without sufficient in-house legal expertise, because they offer an indication of how to comply with the GDPR[87]. They can provide guidance on any aspect of the GDPR, including the identification and assessment of risks, and on best practices to mitigate the risk[88]. During the data protection impact assessment, compliance with a code «shall be taken into due account in assessing the impact of the processing operations»[89]. Adherence to an approved code «may be used as an element by which to demonstrate compliance with the obligations of the controller»[90]. It is one of many relevant factors for supervisory authorities to take into consideration when they decide whether an infringement should be sanctioned[91].

Here, too, the notion of risk is used to operationalise the application of the GDPR. In bringing the GDPR from theory to practice, codes of conduct should «calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons»[92].

Under the Directive, authorities were asked to seek the opinions of data subjects or their representatives in relation to codes of conduct[93]. The recitals of the GDPR also grant individuals a role in this process, but — in keeping with the overall shift

85 See e.g. B.-J. Koops, *The Trouble with European Data Protection Law*, in «International Data Privacy Law», vol. 4, 2014, pp. 250-261.

86 GDPR, art. 40(5).

87 P. De Hert, V. Papakonstantinou, *The new General Data Protection Regulation: Still a sound system for the protection of individuals?*, in «Computer Law & Security Review», vol. 32, 2016, p. 192.

88 GDPR, recital 77.

89 GDPR, art. 35(8).

90 GDPR, art. 24(3).

91 GDPR, art. 83(2)(j).

92 GDPR, recital 98.

93 DPD, art. 27.

towards self-regulation — it is now the drafters of the code who «should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations»[94].

5. Conclusion

Data protection law arose to address the rise of computers in both the public and the private sector. It is ever more pertinent today that both sectors are regulated. Data is shared between the two sectors, and both use personal data for "dataveillance". The GDPR rightly treats both government activity and corporate activity as potential sources of privacy invasions. It regulates the processing of personal data through a number of material and procedural rules, the latter of which accord decisional competence to three actors in particular: supervisory authorities, data subjects, and controllers. These actors play a role in the decision whether or not a certain processing operation is permissible, or whether it constitutes an undue encroachment upon the private sphere of the individuals whose data is being processed. By focussing on the grey area between what is clearly private (falling under the household exemption) and what is clearly public (falling outside of the notion of personal data), data protection law accords these actors a say in drawing and re-drawing the boundary between the public and the private.

Early data protection laws sought to remedy the power imbalance created by the use of computers by focusing on their role in society. However, in a "flight from regulatory substance", legislatures quickly emphasized the rights of control of individuals[95]. Marking a new generation of data protection law, the GDPR attempts to provide more substantive protection through a number of extensive meta-regulatory accountability obligations[96]. With the focus on the controller's accountability and the risk-based approach, the GDPR awards a certain discretion to controllers to make decisions about the legitimacy of their processing operations. We do not have one big brother to watch over privacy. Instead, we rely on the very entities which are liable to "misuse" data to regulate themselves under the watchful eye of both supervisory authorities and individuals.

It is pertinent to speak of self-regulation to the extent that controllers set their own norms regarding what counts as (too high) a risk to the rights and freedoms of individuals, i.e. regarding the proportionality of their processing operations. Self-regulation has a number of benefits. It can make use of the knowledge and expertise of controllers themselves[97]; it is a flexible means of regulating, as self-regulatory standards are more quickly updated than "hard law"[98]; and it can cover

94 GDPR, recital 99.

95 V. Mayer-Schönberger, *Generational Development of Data Protection in Europe*, cit., pp. 230-231.

96 C. Quelle, *The 'Risk revolution' in EU Data Protection Law*, cit., pp. 11-16.

97 R. Baldwin, M. Cave, M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, Oxford 2012, p. 139.

98 C. J. Bennett, *Regulatory Privacy: Data protection and Public Policy in Europe and the United States*, cit., pp. 155-156.

the "grey areas" with regard to which there is no authoritative decision on how to act[99]. Thus, it can cover those questions about legitimacy and proportionality which data protection law fails to address.

The risk-based approach does require a certain faith in «the capacity and commitment of the corporation to self-regulate in the public interest»[100]. Controllers simply may not have the resources to put in place a proactive risk management system, and they may also lack a commitment to the values which are deemed to be in the public good. How do we regulate tax authorities which structurally prioritize the aim of tax collection over data protection? Or digital service providers which do not think privacy is a social norm?[101] Controllers may be more inclined to take privacy seriously if there is a threat that the supervisory authorities would otherwise engage in strict enforcement action, or that the legislature would otherwise impose more restrictive legislation[102]. There is, however, little indication that the EU legislature will pose substantive norms any time soon. The bucket is passed to supervisory authorities, who are faced with a conundrum: should they ban processing operations which are not clearly prohibited under the law?[103]

I want to conclude this article by asking whether the shift towards self-regulation is especially problematic for data protection in the private sector. Despite the omnibus data protection regime, private sector data protection carries different ideological and political underpinnings. Bennett and Raab note that «the paradigm conceives of citizens in their role as individual consumers, perhaps armed with rights, but also as persons whose privacy is deemed a preference to be exercised without regard to any wider social consequences»[104]. Article 35 asks for a "paradigm shift" by placing more responsibility on corporate controllers making away from data subject control. It may very well be that the risk-based approach is a means to avoid a strong top-down presence in privacy regulation. But it is pertinent to ask: is the risk-based approach evidence of a liberal, free market ideology, or of weak legislatures suffering from regulatory capture? The turn towards self-regulation may very well be a failure on the part of the legislature to tame computers and the way in which they are used.

99 C. Parker, *The Open Corporation: Effective Self-Regulation and Democracy*, Cambridge University Press, Cambridge 2002, p. 245. According to Parker, "corporate citizens" need to regulate the grey areas in a "permeable" fashion, following dialogue with stakeholders and regulators.

100 R. Baldwin, M. Cave, M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, cit., p. 152.

101 B Johnson, *Privacy no longer a social norm, says Facebook founder*, in «The Guardian», 11 January 2010, http://www.theguardian.com/technology/2010/jan/11/facebook-privacy, accessed 16 September 2015.

102 I. Braithwaite, J. Ayres, *Responsive Regulation: Transcending the Deregulatory Debate*, Oxford University Press, Oxford 1992, pp. 38-39.

103 C. Quelle, *The Data Protection Impact Assessment. What Can It Contribute to Data Protection?*, LLM thesis, Tilburg University 2015, http://arno.uvt.nl, p. 138.

104 C. J. Bennett, C. D. Raab, *The Governance of Privacy*, cit, p. xxiv.