Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after *Breyer*

*Paul De Hert**

Article 7(f) of that directive precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.
CJEU, 19 October 2016, C-582/14 *Patrick Breyer*, para 62 with ref to CJEU, 24 November 2011, C-468/10 and C-469/10 *ASNEF and FECEMD*

Bind Back the Hound of Technology to Its Cage (Latour and the Idea of Mastery)

My previous contribution in this journal focused on the future of technology.[1] The central question was broad (*How should we, lawyers, approach technology?*). The contribution was short and did not contain any definition of technology.[2] Neither did it critically reflect on important distinctions that could enrich such a definition, for instance, the possible distinction between 'classical' physical technologies and social technologies (like law itself).[3] The bit naïve idea was to say *less* to avoid errors or traps.

Twenty years of selective exposure to literature on ethics and philosophy of technology makes one careful in assuming too much. Who wants to be caught in value judgments derived from ideological or psychological stands on technology without proper basis? On what basis do you assume that technology is good or bad?[4] Why opposing or supporting technologies (for instance as job-killers or job-creators) when discus-

* Paul De Hert is full professor at the Vrije Universiteit Brussels (LSTS) and associated professor at Tilburg University (TILT).
DOI: 10.21552/edpl/2017/1/6

1 Paul De Hert, 'The Future of Privacy. Addressing Singularities to Identify Bright-Line Rules That Speak to Us' (2016) 2(4) European Data Protection Law Review (EDPL) 461-466.

2 See for a definition of technology as 'humanity at work', Joseph Pitt, *Thinking about Technology: Foundations of the Philosophy of Technology* (Seven Bridges Press 2000) 146.

3 See Joseph F Coates, 'Historical lessons from technological disruptions: Will the storm always pass?' (1997) 54(1) Technological Forecasting 111-117.

4 For a critique on technology writings that are 'nothing more than social criticism', see again Pitt (n 2) 146.

sions are often based on a mixture of facts and world views?[5] Take for instance the often heard sceptical line about *the middle class is shrinking partly because of technology*.[6] Tempting to say 'yes, of course', but both assumptions ('the middle class is shrinking' and 'technology is partly responsible') are controversial and in need of empirical backing. I already mentioned discussions about the second assumption. But also the former is open to discussion. That the middle class is shrinking in our century is no hard given. Attention should be paid to differences in times and space and differences between facts and fears.[7] Of course, I am interested in my search for political guidance in strong views *for* or *against* disruptive technologies and players like *Uber*. But, are they disrupting and, if yes, in the short-term or also in the long-term? How to distinguish between minor technological disruptions that will pass and are self-healing in the short- to mid-term and the bigger ones that are often less visible?[8]

Careful to avoid uninformed positioning, I limited myself in my previous contribution to a *Science & Technology Studies (STS)*-flavoured stance about the need for closer scrutiny of existing or novel technologies when considering the role of law and regulation. Detailed accounts of individual technologies allow better assessments of possible ethical dilemmas created by these technologies. Although authors disagree about the degree of moral agency of artefacts or things, most agree that these are more than simple passive instruments. Things influence us and our perceptions about good and bad. Things act and interact. They mediate and impact on our moral understandings.[9] Knowledge about how things do that is not easy. Latour, in particular, criticises every ideal of knowledge and mastery in this area. Technologies simply escape mastery.[10] They are the source of a continuous paradox for humans that praise technology for its functional utility, for its neutrality (neither good or bad) and for it being a means to an end, while these technologies never cease to introduce a history of enfoldings, detours, drifts, openings and translations that abolish ideas like 'function' and 'neutrality'. Latour therefore sheds a critical light on modern humans that have acquired the habit to dominate but fail to see that there are no masters anymore, no clear distinctions between means and end that would allow to identify crazed technologies and 'to bind

5 See on the divergent views on technology and the difficulty for society to decide on possible actions, Sara Baase, *A Gift of Fire: Social Legal, and Ethical Issues in Computing* (4th edn, Pearson 2012) 496.

6 Cf 'America's middle class has shrunk to just half the population for the first time in at least four decades as the forces of technological change and globalization drive a wedge between the winners and losers in a splintering US society' (Sam Fleming and Shawn Donnan, 'America's Middle-class Meltdown: Core shrinks to half of US homes' (*Financial* Times, 9 December 2015).

7 'The middle class is shrinking' thesis is famously defended for the United States by Charles Murray, *Coming Apart: The State of White America, 1960-2010* (Random House USA Inc 2012) 416. Some of the findings are contested. See about a 'middle-class uprising rather than a 'middle-class meltdown' Mark Perry, 'America's middle-class has been shrinking, but it's because so many middle-income households have become better off' (*AEI*, 17 April 2016) <https://www.aei.org/publication/americas-middle-class-has-been-shrinking-but-its-because-so-many-middle-income-households-have-become-better-off/> accessed 3 March 2017. Moreover, there are signs that the evolution is not necessarily irreversible and not necessarily happening everywhere to the same degree. See, for instance, on the catching-up of countries in Europe with a small middle class before the last economic crisis, Daniel Vaughan-Whitehead (ed), *Europe's Disappearing Middle Class? Evidence from the World of Work* (Edward Elgar 2016) 672.

8 Cf Coates (n 3).

9 About some form of agency of technology and technical artefacts, see Bruno Latour, 'Where are the Missing Masses? Sociology of a Few Mundane Artefacts'in Wiebe Bijker and John Law (eds) *Shaping Technology – Building Society. Studies in Sociotechnical Change* (MIT Press 1992) 225–59; Hans Achterhuis, 'De moralisering van apparaten'(1995) Socialisme en democratie 3-11. See more in general Peter Kroes and Peter-Paul Verbeek (eds), *The Moral Status of Technical Artefacts* (Springer 2014) 248.

10 Bruno Latour, 'Morality and Technology The End of the Means' (2002) 19(5-6) Theory, Culture & Society 247–260.

back the hound of technology to its cage'. Morality and technology interact, often in unpredictable ways, and there is a need to conceive another history, another reassembly of morality and technology.

How Latour conceives this reassembly in practice is not clear. A process with openness for predictable and unpredictable outcomes could bring about the necessary dignity of both morality and technology, whereby we renounce the idea of putting the first on the side of means and the second on the side of ends. Latour is no believer in contemporary mantras such as more transparency,[11] or more accountability, assessment and evaluation of options. Wrongly applied, these approaches would lead us again to the impossible ideal of mastery and knowledge of things.

Google Glass and the Futility of the Zero Question (Verbeek's Internal Approach)

Verbeek's writings on technologies suggest more familiar ways to approach them.[12] This author strongly advocates technology-specific assessments, starting as early as possible to assess possible impacts and foreseeable or less foreseeable ethical dilemmas.[13] Verbeek favours Aristotelian *phronesis*. The relation between technologies and ethics is one of mediation, not one of dependence and opposition. Denying that men and technology co-exist is not an option, and neither is denying our faculty of considering critically this relationship with technology. Starting point is the fact that a given technology exists and that the connection with humans is therefore already existing.

Fascinating is Verbeek's rejection of the zero question, the question whether we want or not a certain technology. The question is uninteresting in practice and in principle. It seldom leads to a *no* and almost always to a *yes but under certain conditions*. More fundamental is the lack of sense to ask this question of the acceptability of technology, when a technology has already been invented and by its sheer existence changed our world and our understandings.
More straightforward is the *how* question: how to shape the human condition in its interaction with a concrete technology? The *how* question ('how do we want to embed technologies in our lives') goes beyond the *yes* or *no* and opens up critical interrogations about the way forward with technologies.[14]With this understanding designers, policymakers and users can then move on.

One of the examples given by Verbeek is the *Google Glass*, a small wearable computer capable of giving additional information on surrounding things and persons. The

11 'to look for transparency in matters of technology, what a paradox!'

12 Peter-Paul Verbeek, *Op de vleugels van Icarus* (Lemniscaat 2014) 192.; Peter-Paul Verbeek, 'De Vleugels van Icarus'(2013) 23(2) Ethische Perspectieven 108-123; Peter-Paul Verbeek, *What Things Do. Philosophical Reflections on Technology, Agency, and Design* (Pennsylvania State University Press 2005) 264.

13 More general technology-assessments methodologies are rejected as inaccurate. Every new technology and every new development with regard to existing technologies calls for new critical ethical assessment.

14 Cf Verbeek, 'De Vleugels van Icarus' (n 12) 116.

invention is there, hence the futility of the question whether we want the product or not. Verbeek defends an 'internal' confident approach to ethical interrogation of technologies: they are already there so let us try to understand how we want to live with them. Instead of looking for risks, out of distrustful motives, we should actively interrogate our use and relationships of technologies. Ethics as accompanying technology development rather than judging it from a distanced and disconnected vantage point. Concretely, we will have to look at how people use *Google Glass* and what kind of problems appear. *If* the problem turns out to be the asymmetry with the watched person not knowing whether he is scanned or not, then designers should or could foresee a light that signals scanning activity. Or *scanning* could only be made possible after at least five seconds of explicit staring. Doing nothing, without any critical assessment, is not an option. There is an end obligation for policy makers to see to it that *Google Glass* is well embedded in our society, an obligation that can only be fulfilled through experimentation and asking the right empirical questions: what kind of information should be made available via *Google Glass*? Who decides about what should remain private or not? In what situations should the glasses be taken off? (like exams), etc.

The Idea of Bright Lines Revisited?

In my previous contribution, I insisted on the need to draw clear bright lines to distinguish between legitimate and illegitimate use of technologies. How does this relate to Verbeek's 'internal' ethical approach? These bright lines can (or should) be the outcome of a *how* exercise, not of zero exercise. The basis of this exercise should always be close scrutiny and observing, preferably as early as possible and preferably on a continuous basis: what are specific technologies doing? How are we reacting to their existence and what kind of uses are developed (foreseeable and unforeseeable)? Abstract scrutiny usually fails to have an impact. Problematic aspects are an undeniable part of this broader interrogation. The focus then should be on concrete (not imaginary) wrongs that need to be concretely approached.

Programming *Google Glass* in such a way that unnoticed scanning is not possible expresses a clear bright rule that could either be built into the design or into legal regulations (or both). When these bright rules are transgressed appropriate legal norms should allow for remedy. Seeking for technology-neutral language in defining legal wrongs should not be a first priority and is in fact counter intuitive in the light of the need for technology specific assessment discussed above.[15] Proposed possible measures like adding an alarm light to the glasses that inform persons when the computer

15 A link could be established between these positions and Stephen Toulmin's approach to logic and ethics. This philosopher is well-known for his rejection of the abstract and his insistence of the limitations of modernistic programs, be it ethically or aesthetically or epistemologically that pretend to be able to disconnect practices and experiences from their particular contexts and to obtain results by applying universal, abstract principles. What is needed is not only episteme (reflexive deductive reasoning) but also logic to become more empirical and historical and more practical wisdom (phronesis) that allows to develop a sensitivity for particularities and to enrich. See Stephen Toulmin, *The Uses of Argument* (Cambridge University Press 2003) 247; Albert Jonsen and Stephen Toulmin, *The Abuse of Casuistry: A History of Moral Reasoning* (University of California Press 1988) 420 and Stephen Toulmin, *Cosmopolis: The Hidden Agenda of Modernity* (University of Chicago Press 1990) 228.

is scanning are examples of bright line rules that are technology specific and aimed at better embedding technology. I gave similar examples with regard to biometrics in my previous contribution.

Of course, there are examples of bright line rules that simply outlaw certain technologies and innovations. A fine example of a line draw as a response to the zero question is contained in Article 3 of the EU Charter on Fundamental Rights (EU Charter) prohibiting, amongst others, reproductive cloning. Such outlawing of practices and technologies sends a strong message and it is hard for me to imagine a society that could exist completely without this technique. Important however for the kind of critical coexistence we need to continue with technologies, are clear messages about the *how*. Other illustrations that come to mind are 'No drone without a license' and 'no surveillance power without a warrant'.

The Need for Experimentation Before Regulating (Baase)

The regulatory strategy that I have in mind is not only based on the idea of specificity of the language used and specificity of the object of regulation, but also on Verbeek's idea of experimentation (*above*). Sara Baase connects the idea of experimentation with a specific role for law.[16] Experimentation allows using law only as a last resort. This is the right way to proceed, Baase notes, since laws are not to be compared with personal (consumer) choices and organisational policies about technologies. Laws impose decisions by force on people who did not make them. 'Arguments for passing a law should be qualitatively different from reasons for adopting a personal or organizational policy'.[17] It makes therefore sense, Baase observes, that laws lag behind technology.[18]

This insistence on having the time to confront technologies contrasts starkly with Collingridge' alarming dilemma about law always lagging behind technological developments.[19] The ideal of mastery of technology at work behind this, and similar messages of technology-alarm, can be challenged on several grounds. Some room for experimentation is not necessarily a sign of weakness but allows time for proper analysis, self-understanding (as humans that relate to technology) and understanding of the technology.

16 Sara Baase, *A Gift of Fire: Social Legal, and Ethical Issues in Computing* (Prentice Hall 1997) 382. There is a more recent fourth edition by Pearson from 2012 (n 5). This book came to my attention via the (descriptive) review of Joseph S Fulda, 'A Gift of Fire: Social Legal, and Ethical Issues in Computing. Book review'(2000) 2(4) Ethics and Information Technology 241-247.

17 ibid Baase, 14-15.

18 'It takes time to recognize the new problems, consider possible solutions, think and debate about the consequences and fairness of various proposals, and so on. Once a law is passed, it virtually halts experimentation with alternative solutions and reduces competition and diversity of options. A good law will set minimal standards that can apply to all situations, leaving a large range of voluntary choices. Ethics fills the gaps between the time when technology creates new problems and the time when reasonable laws are passed, and ethics fills the gap between general legal standards that apply to all cases and the particular choices that must be made in a specific case' (ibid Baase, 340).

19 I briefly discussed this dilemma in my previous contribution: controlling a technology is difficult in its early stages because not enough is known of its possible or probable effects, and it is also difficult once the technology is well-developed because by then intervention is expensive and drastic.

Taking time to answer the *how* question does not equate *laissez faire*, although the risk is not imaginary.[20] Baase's discussion about search engines is fascinating.[21] When search engines emerged in the 1990s and allowed to search for names, they took by surprise all those that participated in newsgroups, often about sensitive issues. Before search engines emerged, the likelihood of posted materials being read by a great many was small. Baase sees the problem, but defends *laissez faire and* puts the burden on the individual that posts data: search engines are now here (whether we think they should be or not) and Internet checking on persons (for instance, a prospective employee) is not a wrong. [22]

Verbeek would qualify this attitude as *flying too high*, as uncritically embracing technological developments at the cost of sacrificing what makes us human. In his view, there is cowardice in *no*-saying to technologies, while there is recklessness in lightheaded *yes*-saying to every innovation. Baase's positon on search engines can qualify as flying too high, but it could also be understood as flying at the right height because of its American perspective. It is well possible that experimenting with search engines on both sides of the Atlantic gives different outcomes due to different factors.[23] The outcome of our European process of experimenting with search engines is well-known and has taken the form a right to de-list. This right, first recognized in the 2014 European Court of Justice (CJEU) *Google* decision, has been incorporated in the General Data Protection Regulation (GDPR) that will replace Directive 95/46/EC and find immediate application across the EU on 25 May 2018. The right allows individuals to have links suggested by search engines relating to them removed. The right is already in place and the reception is enthusiastic.[24]

Data Protection as a Regulatory Strategy for the Future?

Sustained focus, permanent assessments, understanding of paradoxes created by technology, faculty to experiment. Where does this bring us in the field of law? I wrote in my previous contribution that the data protection architecture can help us in this task, preparing the grounds for a more general political and social discussion about possible or probable effects, about undesirable applications and about the framing of desired applications. European data protection law, as shaped in the 1995 Directive and the 2016 Regulation, could, to a certain degree, qualify as an example of 'a good law' in Baase's terms: a law that sets 'minimal standards that can apply to all situations, leaving a large range of voluntary choices'.

---

20 Baase's book contains some *laissez faire* examples about the acceptability of certain of technologies that are simply inacceptable, at least for ears tuned to the European human rights message about governments having a final responsibility in creating a human rights respectful framework for technology. Cf Paul De Hert, 'Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law' in Daniel Guagnin et al (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012) 193-232.

21 Baase (n 16) 344.

22 ibid.

23 See about transatlantic differences in balancing privacy and free speech and in protection of public aspects of one's life, Ronald J Krotoszynski, Jr, *Privacy Revisited: A Global Perspective On The Right To Be Left Alone* (Oxford University Press 2016) 292.

24 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) EU:C:2014:317.

There is some room for experimentation in data protection law (for instance via impact assessment exercises and prior notice). Although European data protection law hesitates between abstract and detailed standards, the spirit of this set of rules remains one of flexibility and adaptability. Most provisions formulate or apply broad principles, but do not specify how they are to be implemented in detail. Even in the provisions on sensitive data there is nothing that comes close to a veto to certain technologies or processing activities. Protection of personal data has been recognized as a fundamental right in the 2000 EU Charter, but the phrasing has been done carefully and again without outlawing the idea of processing of personal information.[25] Article 7 of the Directive provides no less than six cases in which the processing of personal data can be regarded as being lawful.

A key indication of the flexibility is of course the case or ground provided for in Article 7(f) of the Directive, which is reproduced in the GDPR.[26] Article 7(f) is the last of six grounds for the lawful processing of personal data and it is without any doubt less constraining than the other grounds. It allows to process data without consent or a legal basis, solely based on the legitimate interests of the controller, 'except where these interests are overridden by the fundamental rights and interests of the data subject'. *Laissez faire* has never been more elegantly phrased.
We are miles away from the privacy logic as expressed in Article 8 of the European Convention on Human Rights (ECHR) with its insistence on the need for restrictive interpretation of exceptions to rights, the need for a legal basis provided for by law and proportionality testing. In the literature, it was advanced that we need a rights perspective and a slimming down of Article 7(f), to do justice to the fundamental rights status of data protection.[27] But the tide is not going that way.

The CJEU *Patrick Breyer* Judgment (2016): Technology-Friendly Definitions

The 2016 *Patrick Breyer* judgment of the CJEU was delivered after a request for a preliminary ruling concerning Article 7(f) of the Directive. [28] The request had been made in German legal proceedings concerning the registration and storage by German public authorities of the Internet protocol address (IP address) of visitors, in this case of Patrick Breyer, a Pirate Party politician, when he accessed Internet sites operated by German Federal institutions.

---

25 Cf McKay Cunningham, 'Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm'(2014) 2(2) Groningen Journal of International Law 115-144, 115.

26 It provides that: 'Member States shall provide that personal data may be processed only if: ...(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

27 Federico Ferretti, 'Data Protection And The Legitimate Interest Of Data Controllers: Much Ado About Nothing or The Winter Of Rights?' (2014) 51 Common Market Law Review 843–868, 845.

28 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* (2016) ECLI:EU:C:2016:779,. See Tim Hickman et al, 'IP addresses and personal data: Did CJEU ask the right questions?' (2017) 145 Privacy Laws & Business 32-34; Fabian Niemann and Lennart Schlussler, 'CJEU decision on dynamic IP addresses touches fundamental DP law questions' (*Bird & Bird*, 21 October 2016) <https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions> accessed 3 March 2017.

Breyer is firstly about the definition of personal data (the second part about Article 7(f) will be discussed *below*). It is secondly about clarifying this central notion in European data protection law. In *Scarlet*, the CJEU had already found that the collection of IP addresses qualifies as collection of personal data when it is done by Internet service providers such as Scarlet.[29] This time, in *Breyer*, the Court had to answer the question whether dynamic IP addresses of website visitors constitute personal data for website operators and other online media service providers.[30]
The answer was like in *Scarlet* - again *yes*, which is an important interpretative step, since identification is more difficult when done by website operators. They need the help of Internet service providers to obtain additional data, other than the IP addresses, necessary to identify the individual. So even if an IP address, and in particular a dynamic IP address, does not bring you directly to an individual and you need third parties to supply you with additional information, data protection law applies to the website operators.

To this, the CJEU adds an important caveat: the possibility to combine the original data with this additional data must constitute a 'means likely reasonably to be used to identify' the individual. This legal *doublespeak* implies that when parties are collecting IP addresses, a case-by-case analysis is needed of law and context to determine whether these IP addresses are to be considered personal data. Possibly, it can then be found that certain IP addresses in the hands of certain actors in certain legal or practical contexts are *no* personal data when there are legal or practical obstacles to identification so that the risk of identification appears in reality to be insignificant. In the case at hand, the risk and intention was there, since the collection of IP addresses by the German public website operators was done to bring criminal proceedings against cyber criminals attacking their websites (after identification with the help of Internet service providers).

I want to make three observations about *Breyer's* definitional part.[31] *Firstly,* the Court could have gone much further in creating a full equation between IP addresses and personal data by creating a general assumption that one equals the other and that data protection applies to *all* collection of IP addresses. Not creating a bright line rule in favour of an absolute approach, but allowing relativity like the Court does, allows for more flexibility and will create more leeway for certain anonymisation and Big Data practices that 'help' actors to stay out of the scope of data protection law.[32]

---

29 Case C-70/10 *Scarlet Extended v Sabam* (2011) ECLI:EU:C:2011:771.

30 See para 16 of the *Breyer* judgment: 'it is clear from the order for the reference and the documents before the Court that internet service providers allocate to the computers of internet users either a 'static' IP address or a 'dynamic' IP address, that is to say an IP address which changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider'.

31 For a full rejection of the findings of the Court and the hypothesis that, especially with the GDPR, an even more narrow definition will impose itself, see Hickman et al (n 28) 34.

32 On this distinction between 'subjective/relative approach' and 'objective/absolute' approach, see para 25 of the judgment. See also Niemann and Schlussler (n 28).

Secondly, the CJEU seemingly applies a narrower approach to the concept of personal data compared to what many European data protection authorities (DPAs) required in practice.[33] The judgment mentions academic disagreement about this issue (paragraph 25), but is silent about the position of DPAs on the issue.

Thirdly, there is the chronology of things and the question about the useful length for experimentation. The discussion about IP addresses has been around for three decades. Only recently - in 2011 (*Scarlet*) and 2016 (*Breyer*) - was high authority guidance given. My impression is that this longer period has allowed for some necessary incubation of the minds in favour of the data protection logic (to understand the importance of IP addresses within the architecture), and in the same time has allowed to open up both the Directive and the Regulation for the (more recent) concerns of private and public actors for Big Data and cyber security gains.

Breyer Continued: No National Bright Line Rules for the Concept of Legitimate Interest

Breyer was delivered after a request for a preliminary ruling concerning Article 7(f) of the Directive. Again there was a problem with academic disagreement at the basis of this part of the request. Section 15(1) of the German *Telemedia Act* only allows collection and use by a service provider of user's personal data on the basis of consent or when the information are necessary to facilitate the specific use of the website/media service or to charge the user for it. Section 15 does not explicitly foresee cyber-security measures. The referring German court did not see any problem for website operators to collect IP addresses in view of combatting possible cyber-attacks, but was confronted with a dominant restrictive reading of Section 15 amongst academics. This restrictive reading 'would prevent the storage of IP addresses from being authorized in order to guarantee in a general manner the security and continued proper functioning of online media' (paragraph 28). Indeed, strict application of the Section 15 criteria implies that data must be deleted at the end of the period of consultation concerned and that keeping this data any longer for security reasons is not justified. This restrictive understanding was, at least for the German court, reason for concern since it excludes *ad-hoc balancing* and precludes a justification based on legitimate interests (Article 7(f) of the Directive).

The reaction of the CJEU was foreseeable. In line with *Asnef* (2011)[34] it saw no reason to allow Member States to go outside the Directive in the name of fundamental rights. The German Act, in its strict interpretation, would make impossible a proper use of the Article 7(f) criterion and would therefore deny to German operators the flexibility of the Directive. That would negatively affect one of the two main purposes of the Directive: the protection of private life *and* the free movement of personal data within the

33 ibid.

34 Cf Cases C-468/10 and C-469/10 *ASNEF and FECEMD* (2011) ECLI:EU:C:2011:777.

EU through a harmonisation of data protection laws (paragraph 58). In an important paragraph 62, the Court excludes any change to the spirit of Article 7 and any categorical outlawing of processing of personal data to the detriment of the balancing spirit of Article 7(f).[35]

As said, the precedent was *Asnef,* a judgment about the validity of a Spanish Royal Decree implementing the Spanish data protection Act (Organic Law 15/1999). This Decree added to the legitimate interest-ground, that processing on this ground is only lawful if the fundamental rights of the data subject are not prejudiced *and* if the data appears in public sources. The Spanish idea was simple: no *legitimate interest* processing is allowed with data appearing in non-public sources, unless consent is obtained. The CJEU did not like the taste: it banned both Member States adding new principles relating to the lawfulness of processing *or* imposing additional requirements.[36] The only things Member States can do is adding *precisions*,[37] but only in accordance with the objective pursued by the Directive of maintaining a balance between the free movement of personal data and the protection of private life. The Court understands why Spain is more restrictive with regard to non-public data and recognizes that this could be a factor when doing the *legitimate interest* balancing. However, when national data protection rules exclude all balancing in the case of public source data, then this is no longer a *precision* within the meaning of the Directive.[38]

The relevance of these paragraphs from *Breyer* and *Asnef* is self-evident for our purposes. Clarifying data protection via democratic deliberation in Member States becomes virtually impossible. From a rights perspective, there is nothing but praise possible for the Spanish and German concern to regulate well and create clarity about the roles and duties of the different actors involved in Internet activity. However, that is not the perspective of the EU data protection law, as understood by the CJEU. Whatever the outcome of democratic deliberation about processing activities might be in Member States, the six justifications for lawful processing (including the justification based on legitimate interests) prevail and so does applying them in a general way.

This *pro Europe* position is of course not encouraging critical interrogations by humans who live with technologies and try to make sense of it. Cyber attacks are a novel phenomenon. My preference goes out to a more classical approach at this point: conveying the German representatives in the Federal Parliaments and asking them to reconsider Section 15(1) of the *Telemedia Act* in order to make effective cybercrime possible or *not*. Considering what kind of data is collected by the German public authori-

35 This paragraph opens my contribution (see *above*).

36 *Asnef* (n 34) para 29-32.

37 art 5 of the Directive authorizes Member States to specify the conditions under which the processing of personal data is lawful, within the limits of art 7, inter alia.

38 *Asnef* (n 34) paras 40-47.

ties in the name of preventing attacks to their websites,[39] the critical interrogation would ideally include a reflection about the right to obscurity in particular of users of public websites.[40] We can avoid visiting a commercial website, but is there avoidance possible of public websites?

The impact of the CJEU mainstreaming policy is considerable. German authors foresee that original German protective measures will follow suit, for instance those with regard to the admissibility of profiling in Germany.[41]

Thinking this through, one is amazed by some of the consequences. If the Working Party 29 assembly of EU national DPAs would issue a recommendation with bright line rules comparable to those in the *Telemedia Act*, there would not be a problem, since there would not be formal *hard* law rewriting of Article 7, but soft law *and* moreover an EU top-down soft law! In fact, there is such a recommendation, and one of considerable quality, with an insistence on steps to follow to carry out the Article 7(f) balancing and, in addition, 26 examples with case specific recommendations. However, faithful to their ethos as identified in my previous contribution ('data protection authorities will never recognize the limits of data protection law and never ask for legislative clarification of bright lines'), the recommendations are not formulated in a hard, imposing tone, although they could easily be transformed in sector and technology specific rules.[42] European data protection at its best, open-ended, fuzzy, negotiable and weary of sending out clear messages about meaningful issues. Happy?

The Idea of Legal Certainty In EU Data Protection Law (Radbruch and Kohr)

The value missing is of course legal certainty and all its benefits. Out of respect for the German and British legal system - to name only two systems known for their attachment to legal certainty - it is useful to recall Radbruch on moral aspirations of legal systems. Radbruch insisted on equality before the law and legal certainty as indispensable moral requirements without which a legal system cannot be called law. [43] Together with purposiveness of the law ('does a measure serve the public benefit?') they create Radbruch's famous justice calculus. Striking is his priority given to legal certainty

39 These authorities, in the name of preventing attacks to their websites, store information on all access operations in log files. The information retained in the log files after those sites have been accessed include the name of the web page or file to which access was sought, the terms entered in the search fields, the time of access, the quantity of data transferred, an indication of whether access was successful, and the IP address of the computer from which access was sought. See *Breyer*, para 14.

40 See Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) 2(2) Groningen Journal of International Law 33-54, 52: This 'right' to obscurity 'should place the burden on service providers and technology manufacturers to create technology that provides users with the possibility to maintain the obscurity of certain information if they choose to do so'.

41 'The judgment may further have a massive practical impact on the admissibility of Profiling in Germany. Under the current regime, Profiling is subject to very strict rules in Germany – arguably the strictest in the EU. According to section 15 (3) of the German Telemedia Act Profiling may (at least according to the prevailing legal view in Germany) only take place (i) if it is covered by the users' consent, (ii) if the respective data is anonymised, or (iii) if – but only for certain limited purposes – it is undertaken on basis of pseudonymised data (subject to further requirements). Even though the CJEU did not expressly comment on these rules, the reasoning of the judgment can generally also be applied to this provision' [Niemann and Schlussler (n 28)].

42 See Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (9 April 2014) 68.

43 Gustav Radbruch, 'Statutory Lawlessness and Supra-Statutory Law (1946)' (2006) 26(1) Oxford Journal of Legal Studies 1–11.

within the calculus. Without it being a decisive value, it has an elevated status ('any statute is always better than no statute at all, since it at least creates legal certainty'). Legal certainty should be understood as an intrinsic part of justice itself:

> That the law be certain and sure, that it not be interpreted and applied one way here and now, another way elsewhere and tomorrow, is also a requirement of justice. Where there arises a conflict between legal certainty and justice, between an objectionable but duly enacted statute and a just law that has not been cast in statutory form, there is in truth a conflict of justice with itself, a conflict between apparent and real justice. (…) The conflict between justice and legal certainty may well be resolved in this way: The positive law, secured by legislation and power, takes precedence even when its content is unjust and fails to benefit the people, unless the conflict between statute and justice reaches such an intolerable degree that the statute, as 'flawed law', must yield to justice.[44]

With this in mind, one could ask the CJEU whether, for instance, the Spanish decision to outlaw processing of non-public data without consent *reaches such an intolerable degree that the statute, as 'flawed law', must yield to justice?* I do not think so and deplore the Court's inability to see applications of principles in very defendable cases (like non-public data) as *precisions*.

The CJEU's position to give primacy to EU law and to object to balancing of interests being done by Member States prioritizes one kind of abstract legal certainty ('EU law is the same in all Member States') to the detriment of Radbruch's understanding of legal certainty requiring that guidance is given to subjects to orient their behaviour here and now *and* tomorrow. The CJEU seems to deny a very simple truth that (too) abstract standards, may not be able to protect personal data in practice.[45] Just attempts by national legislators to implement these standards in specific context (such as the one envisaged by the German *Telemedia Act* and the Spanish Royal Decree) are rejected in the name of uniformity and the justice of making balancing possible wherever and whenever. Thus, the CJEU closes the doors for Member States that show legal ambition to build up incremental, graduated and practical legislation to better achieve the goals of data protection by adding sector specific guidance (Germany) or by delimitating better the broadly formulated principles for lawful processing (Spain). [46] Largeness, Leopold Kohr observed in 1957, seems the real cause of our misfortune.[47] The approach of the CJEU shows that the EU comes at a price. Local communities can bring the problems they encounter under control, vast multitudes cannot:

> What matters in the affairs of a nation, just as in the affairs of a building, say, is the size of the unit. A building is too big when it can no longer provide its dwellers with the ser-

44 ibid 7.

45 Christopher Kuner, 'The European Union and the Search for an International Data Protection Framework' (2014) 2(2) Groningen Journal of International Law 52.

46 Cf Cunningham (n 25) 115.

47 Leopold Kohr, *The Breakdown of Nations* (EP Dutton 1957) 171-172.

> vices they expect (…) A nation becomes too big when it can no longer provide its citizens with the services they expect - defense, roads, posts, health, coins, courts, and the like-without amassing such complicated institutions and bureaucracies that they actually end up preventing the very ends they are attempting to achieve, a phenomenon that is now commonplace.[48]

Size governs and the CJEU is playing it hard with its *pro EU* agenda (if needed at the detriment of data protection fundamental rights dimension). To succeed at this, the Court works double shifts and is firing one judgment after another, sometimes about the essentials, sometimes about details instructing us about data protection as a fundamental right *and* as a regulatory set of technical legal rules. A similar double gun is used in other areas of EU law and compared to, for example the US Supreme Court, the quantitative output by Luxembourg is amazing. Almost everything in the EU is now done by the Luxembourg judges, writes Spahiu, who sees a mechanism at work where power *and* work is shifted from the Brussels officials to judges.[49]

Real or not, the risk taken by the CJEU is considerable. There is of course the issue of feasibility. Take for instance the IP address discussion, around for at least three decades, before the Court solved the matter (for the time being) in *Scarlet* and *Breyer*. Will the Court keep up? Will national courts ask the right questions to the Court? How fragile and lonely this (partly self-created) position of the CJEU! Why waiting for a European Court decision on acceptable profiling, if the German legislator has looked at the matter and has taken regulatory options that could inspire actors in other countries. Whether the Court is giving the right kind of legal certainty by smashing Member States attempts to apply the data protection principles is in my view questionable. Paraphrasing Kohr (*above*): the data protection space created within the EU might not be capable of providing the EU citizens with the services they expect, not even with the help of 'complicated institutions and bureaucracies' at hand.

Puzzled by Data Protection Authorities (Bonnor) and the Need for Performance Measuring

The complicated bureaucracies I have in mind are, of course, the national DPAs and their European gathering (now the Working Party 29 and in the GDPR-future the European Data Protection Board). These supervisory bodies play multiple roles, including education, consultancy, provision of policy advice, international coordination, as well as enforcement of regulation.[50] In a previous contribution, I compared them with *Don Quixote*, mounting his horse at the sight of every new technology. I did not question this role as technology spotter but saw more difficulties with the

48 Kirkpatrick Sale, 'Foreword to *The Breakdown of Nations*', ix.

49 About this process of judicialisation or *Eurolegalism,* Irma Spahiu, 'Courts: An Effective Venue to Promote Government Transparency? The Case of the Court of Justice of the European Union'(2015) 31(80) Utrecht Journal of International and European Law 5-24, DOI: http://dx.doi.org/10.5334/ujiel.ct.

50 David Barnard-Wills, 'The technology foresight activities of European Union data protection authorities'(2017) 116 Technol Forecast Soc Change 142-150.

acquired role of technology regulator: identified non-justified political delegation with national parliaments not taking up their national role of regulating new challenges created by technologies 'out of respect for the roles of the data protection authorities'. My discussion of the CJEU's *Patrick Breyer* judgment (*above*) aimed to highlight how this mechanism is reinforced by the *bigger Europe* agenda of Luxembourg.

So the future of data protection law partly depends on the DPAs. They play multiple roles and pop up in ongoing technology debates. Let us quickly make a small comparison with other newcomers in the legal political arena: the ombudsmen. In 2003, Bonnor identified three positions or views with regard to the relatively novel phenomenon of ombudsmen: there are the puzzled, the sceptics and the unsurprised.[51] He furthermore quotes a colleague who, in a speech to an ombudsman world congress, stated that, if Montesquieu had known of the ombudsman institution, he would have talked of four rather than three branches of government.[52]

This way of presenting things invites us to allow surprise and puzzlement. The institute of the ombudsman is not so distanced from the DPAs. Both are independent authorities (with their own powers and responsibilities) and both are organisationally separate from government.

Bonnor looks in detail at the ombudsman in Sweden and in Denmark. In both countries the ombudsman has been a source and driver of public law (legal source function), especially in areas with very little relevant legislation and in particular in areas concerning freedoms, legal certainty as well as public access to document.[53] The ombudsmen's more flexible and cooperative way of operating, as well as their problem-identifying abilities, have turned them into quasi-autonomous developers of specific fields of administrative activity which other existing mechanisms would not have 'regulated' to the same extent or equally well, Bonnor observes.

Also, in both countries there is a tension between acting with regard to individual complaints (the banal) and acting on general policy issues (the fundamental), with critical voices being raised whenever the ombudsman dared to focus too much on the latter. Neglecting individual complaints is a tempting solution to address workload, but meets very little political understanding.[54]

Interesting also is Bonnor's observation that Swedish and Danish courts take a somewhat 'free approach', sometimes ignoring the work of the ombudsman, sometimes using it.[55] The last observation is of some importance, since we found no discussion of

51 Peter Bonnor, 'Ombudsmen and the Development of Public Law' (2003) 9(2) European Public Law 237-239.

52 ibid 244, with reference to Prof Gammeltoft-Hansen.

53 Bonnor (n 51) 239.

54 ibid 243-246.

55 ibid 260.

the work of DPAs in *Patrick Breyer*, only references to academic controversies (see *above*). Apparently the EU 'complicated institutions and bureaucracies' are not working in tandem.

Bonnor briefly mentions existing discontent about the ombudsmen[56] - similar to the discontent some spread about DPAs - to end his study with a call for more research on these authorities. Out of respect for Montesquieu, there is good reason to voice a similar call with regard to the institutional data protection machinery. We need empirical and sociological research on these authorities, including a tool similar to the EU Justice Scoreboard[57] to measure their performance in all these different roles and their trustworthiness in the constitutional landscape. The existing case law from the European Court on Human Rights regarding the right to an effective remedy (Article 13 ECHR) could help identifying some of the relevant benchmarks.

In that exercise, my attention would go out to the DPAs' ability to explore, engage in dialogue and interrogate new or evolving technologies. David Barnard-Wills' excellent study on technology foresight activities of these authorities show that still a lot of work has to be done, also at the level of the legal mandate, since technology foresight is not, for the most part, an explicitly mandated task. [58] Currently, these mandates as supervisory and enforcement agencies create primarily reactive functions. There are good examples of active technology exploration taken from some Member States, but the authorities in smaller countries lack proper resources to engage in foresight. In general, Barnard-Wills observes, there is still a long way to go to achieve proper public participation in DPA foresight exercises and there is an equally long way to intra-DPA collaboration on foresight.

That is where we are. Data protection in the EU has an open future and its added value depends on the ability of the CJEU to keep up with the number of questions and the ability of the DPAs to tease out our relationship with new technologies, to identify the right problems and come up with recommendations to integrate these technologies in our lives and system of values.

Hopefully, there will be amongst the expected output some room for bright line rule guidance (to technology designers, to users, to regulators) when answering the *how* question (*how to shape the human condition in its interaction with concrete technology*). Democratically imposed or expert imposed, without these bright lines we might be flying too high (uncritically embracing technological developments) at the cost of

56 Such as hierarchy problems; non-legality reviews causing confusion and legal uncertainty; centralisation of deliberations (`one person and a handful of legal advisers'); the absolute discretion to decide which cases to pursue; the separation of powers (primarily the FO), etc.

57 European Commission, 'EU Justice scoreboard' (2016) <http://ec.europa.eu/justice/effective-justice/scoreboard/index_en.htm> accessed 3 March 2017. The EU Justice Scoreboard is an information tool aiming to assist the EU and Member States to achieve more effective justice by providing objective, reliable and comparable data on the quality, independence and efficiency of justice systems in all Member States. Such data is essential to support reforms in national justice systems required to render justice systems more effective for citizens and businesses.

58 Barnard-Wills (n 50).

sacrificing what makes us human and at the cost of legal certainty as a moral requirement to legal systems.

(*to be continued*)