Regulating Big Data in and out of the data protection policy field

de Hert, Paul; Sajfert, Juraj

Published in:
European Data Protection Law Review

DOI:
10.21552/edpl/2019/3/8

Publication date:
2019

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

Regulating Big Data in and out of the Data Protection Policy Field:

Two Scenarios of Post-GDPR Law-Making and the Actor Perspective

*Paul de Hert and Juraj Sajfert**

> There is no sense in studying ideas as if they floated in a kind of intellectual heaven, with no reference to the agents who produce them or, above all, to the conditions in which these agents produce them, that is, in particular to the relations of competition in which they stand towards one another.[1]

Why is Big Data absent in the recent basic data protection documents of the European Union (EU) and the Council of Europe (CoE)? Why not one single reference to Big Data practices - be it to regulate or to prohibit it - in the recent General Data Protection Regulation (EU) 2016/679, the Data Protection Law Enforcement Directive (EU) 2016/680 and the Modernised CoE Convention 108 for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+)? Some actors in the policy field considered Big Data too dangerous and counted on existing data protection principles to tame the beast. Others simply ignored the phenomenon or were not aware of the potential benefits of Big Data for economy and governments (the rendez-vous was missed). Our discussion of no less than six recent initiatives, - standalone laws and soft law instruments - is an indication that Europe is embracing Big Data but is seemingly hesitant to confront Big Data within the classical paradigm (field) of data protection law. Concrete guidance for Big Data practices is now spread over multiple texts emanating outside the data protection field.

I. Two Strategies in Europe to Address Big Data: Inside and Outside the Realm of Data Protection Law

We understand Big Data as the analysis of large data sets in order to find new correlations - for example, to predict business or political trends or to prevent crime - and to extract valuable information from large quantities of data.[2] Big Data can also be understood more loosely as an umbrella term for technological and societal developments that are already taking place (use of profiles, algorithms, cloud computing, machine learning, commodification of data, open access to governmental data, datafication, securitisation and risk society).[3] Today, Big Data is not confined to science and research institutes as it has entered all domains of economic, political and social life.[4]

This contribution looks at the European legal responses to Big Data. Our focus will be on European Union (EU) data protection law, governed by the General Data Protection Regulation (GDPR)[5] and the Data Protection Law Enforcement Directive (LED)[6], and

* Paul de Hert, Professor at the Vrije Universiteit Brussel (LSTS), Belgium and the University of Tilburg (TILT), The Netherlands. Juraj Sajfert, Official of the European Commission. The views expressed in this article are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission. For correspondence: email.

1 Pierre Bourdieu, *On the State: Lectures at the College de France, 1989-1992* (Polity Press 2014) 341.

2 Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales

within the Council of Europe (CoE) by Convention 108+.[7] While skimming through these basic texts, one is amazed by the lack of explicit consideration of the Big Data phenomenon.

Our hypothesis is the following: Europe, to respond to the emergence of Big Data, has deployed two complementary strategies: on the one hand, counting on the vitality of existing data protection principles to frame a new development and thus continuing a principle-abiding approach in reform times (*first strategy*), and on the other, regulatory reform to enable Big Data developments based on a thorough re-evaluation of the regulatory principles (*second strategy*).

Both strategies or approaches co-exist, but are kept separate. The first approach follows the classic realm of data protection law and explains the relative silence of the basic texts on the issue of Big Data mentioned above. The second approach justifies the recent adoption of standalone legislation and soft law instruments both at the level of the EU and the CoE that in one way or another impact the relationship between Big Data and data protection. These initiatives are usually pursued by other than the classical data protection actors (in the EU, this would be DG Justice and Consumers of the European Commission (DG JUST), the LIBE Committee of the European Parliament, the DAPIX Working Party of the Council, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS)).

We will discuss six recent legal initiatives voted at European level and designed to facilitate the adoption of Big Data practices: the Directive (EU) 2019/770 of 20 May 2019 concerning contracts for the supply of digital content and digital services and the European Commission Communication on a data-driven economy;[8] the revised Copyright Directive;[9] the reform of Directive 2003/98/EC on the re-use of public sector information (PSI Directive) by the Open Data Directive;[10] the 2018 EU Regulation on the free flow of non-personal data[11]; the 2015 Payment Services Directive[12] (PSD2) and the development of the Ethics Guidelines for the Artificial Intelligence[13].

Our discussion of the two regulatory approaches and the six policy examples is followed by a reflection

et al (eds), *New Technology, Big Data and the Law, Perspectives in Law, Business and Innovation* (Springer Nature Singapore 2017) 17-42. Big Data is the collection and aggregation of large masses of (publicly, commercially, proprietarily, and/or illicitly) available data from a wide variety of different sources and its analysis, largely in the form of correlation, pattern-recognition, and predictive analysis. So big data is about massive collection and analysis, often secondary analysis or analysis for new purposes, other than those for which the data were originally produced and collected (Ann Rudinow Saetnan, Ingrid Schneider and Nicola Green, 'The politics of Big Data. Principles, policies and practices' in Ann Rudinow Saetnan, Ingrid Schneider and Nicola Green (eds), *The Politics and Policies of Big Data: Big Data, Big Brother?* (Routledge 2018) 1-18. This contribution also contains also a critical discussion of existing definitions, including the commonly used definition of big data as great data volume, data velocity, and data variety (and veracity). For more on definitions, see Bart van der Sloot and Sascha van Schendel, 'Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study' (2016) 7 JIPITEC 110, 112-114.

3 van der Sloot and van Schendel ibid 115.

4 Mark MacCarth, 'In Defense of Big Data Analytics' in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018) 47, 49.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L 119/1.

6 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/ 89.

7 Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28 January 1981, as modernised in the 128th session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018).

8 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a thriving data-driven economy (2014) COM(2014) 442 final.

9 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance) [2019] PE/51/2019/REV/1, OJ L 130/92.

10 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172/56.

11 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance) [2018] OJ L 303/59.

12 Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015].

13 In April 2019, the High-Level Expert Group on Artificial Intelligence (AI HLEG) published its Ethics Guidelines <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top> accessed 18 June 2019. The AI HLEG was established by the European Commission in June 2018 to support the implementation of its Strategy on Artificial Intelligence and to prepare two deliverables: (1) AI Ethics Guidelines and (2) Policy and Investment Recommendations. See on the composition of the expert group with no representatives of the EDPS or the DPA's <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence> accessed 18 June 2019.

on regulatory failure. How unfortunate is the missed *rendez-vous* between new data protection rules and the emergence of Big Data in the 2016 EU reform texts and the 2018 CoE revamped Convention? How unfortunate is the choice to 'deal' with Big Data mainly in specific legislation and soft law instruments?

Before discussing the said approaches in sections 3 and 4 and assessing both their benefits and shortcomings, we first recall some basic ideas behind European data protection law using a Bourdieuan grid in the following section in order to identify the specific actors that are operating within the regulatory landscape.

II. Bourdieu: The CoE and the EU as Interacting Fields

Data protection law is the set of legal provisions that apply to any 'processing of personal data wholly or partly by automated means.'[14] In particular, European data protection law is broad and generic, be it defined at the level of the CoE or the EU. It applies to both private and public sector, including police and law enforcement, with Convention 108+ also stretching out to national security and defence.[15] Its objective is to offer protection to individuals against potential abuses and to regulate trans-border flows of personal data. It lays down the basic principles of data protection,[16] and strict requirements for the processing of special categories of personal data (race, politics, health, religion, sexual life or criminal record).[17] Key in understanding data protection law is furthermore the establishment of supervisory authorities (data protection authorities), the obligations of data controllers and the recognition of data subject rights.[18]

The CoE and the EU are said to be 'products of the same idea, the same spirit and the same ambition', both promoting human rights and sharing the same values.[19] The EU Member States are bound by the provisions of the CoE when they have ratified them, but it is also possible for them to agree, gathered in the Council of the European Union, to standards higher than CoE in the EU legislation.

In Pierre Bourdieu's terms, both organisations can be best understood as autonomous (but often interacting) settings with specific agents, social positions of agents, particular rules and internal dynamics.[20] The specificity of the respective rules and positions explains why comparing both organisations in terms of parameters such as human rights is not an easy task. Comparing the performance of both organisations with general statements is inappropriate. Every policy issue will play out differently and an in-depth analysis of the respective rules and actors, internal and external dynamics is warranted.[21]

14 See, for instance, art 2(1) of Regulation (EU) 2016/679.

15 Convention 108, art 3(1): The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors. The modernised Convention 108 changed the wording of this provision, but not the substance: Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data.

16 In particular the principles of fairness and lawfulness of data processing, the purpose limitation principle (data should be collected for specified, legitimate and explicit purposes and not further processed in a way incompatible with those purposes), the storage limitation principle (data should not be kept longer than necessary) and the data quality and proportionality principle (data should be accurate, adequate, relevant and not excessive). More recently recognised principles (mainly at the European level) the principles of transparency, accountability, data minimisation, and privacy by design. See on these new principles 'The modernised Convention 108: novelties in a nutshell' (May 2018) <https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8> accessed 18 June 2019.

17 See more in the 'Handbook on European data protection law' (Fundamental Rights Agency and Council of Europe, 2018) <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> accessed 18 June 2019.

18 Citizens have the right to be informed that their data is being used in a processing operation. They also have the right to access their data when these have been processed, eg, they can investigate how the processing operation is carried out, whether databases exist, what their purpose is, and who is responsible for the processing. Furthermore, in case the data appear to be incomplete, inaccurate, or processed in a manner that is incompatible with the other data protection principles, the data subject has the right to ask for the rectification, or even the erasure of his data. Data subjects are also entitled to object to the processing of their personal data provided there are 'compelling legitimate grounds'. Finally, data subjects have the right 'not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data', which means that important decisions concerning them cannot be taken solely on the automated processing of data, and that they have a right to actively participate in those very decisions.

19 Rebecca Deruityer, 'Norm and standard setting for the detention of asylum seekers in Europe: The Council of Europe and the European Union as two different stories of a cosmopolitan outlook?' in Antoinette Verhage and Gert Vermeulen (eds), *Mensenrechten en opsporing, terrorisme en migratie* (Maklu, 2017) 105-124.

20 See Bourdieu (n 1).

21 See for a comparison in the area of detention norms, the study of Rebecca Deruyter, *above*. For a comparison in the area of criminal law, see Paul De Hert and Angela Anguinaldo, 'A leading role for the EU in drafting criminal law powers? Use of the Council of Europe for policy laundering' (2019 forthcoming) New Journal of Criminal Law 1-8.

The role of soft law - for instance, its creation and authority - plays out differently in the two organisations. The European Court of Human Rights (ECtHR), one of the most eminent CoE bodies, increasingly refers to soft law standards developed by other CoE bodies (eg recommendations), turning these standards into a sort of '*hardened soft law*' in the CoE's normative system.[22] It is at present not possible to detect a similar development at the level of the EU. Recitals in directives and regulations are one form of EU soft law. They do not always form a coherent whole. At their worst they express wishes by the different negotiating partners about what certain provisions are supposed to mean. Deprived of immediate hard value, they can transform from wish into norm, when the Court of Justice of the European Union (CJEU), responsible for overseeing EU law, refers to one of the recitals in its binding interpretations.[23]

Not only the creation of soft law differs on CoE and EU level. The adoption of hard norms and their decision-making process equally shows more differences than similarities. The CoE is organised as a classical international organisation with a high impact role for agents of executives of the contracting parties who meet in relative isolation to prepare new conventions, whereas the EU has been granted, with the Lisbon Treaty, a more classical model of powers as we know it from domestic law, with a law making role entrusted to both the European Parliament (representing the European demos), the Council (representing the governments of the Member States), and the European Commission as initiator. This rather classical constitutional set-up guarantees more transparency in the decision-making process, although some secrecy is created by the involvement of specific actors like the rotating Presidency of the Council, the Rapporteur and the Shadow Rapporteurs in the European Parliament and the different Council formations (national experts, counsellors and the ambassadors in COREPER - the Committee of the Permanent Representatives of the Governments of the Member States to the EU).[24]

Our contribution opened with a quote from sociologist Bourdieu, taken from his 1989-1992 lectures that insist on going beyond a history of ideas - approach in disciplines such as philosophy *and* law - by opening up to the actors that take up and shape up ideas. Political scientists have understood the message and have applied it not only to states, but also to international relations: they abandoned older approaches to international organisations (such as the EU and the CoE), in favour of political science approaches that study not only these organisations but also their related actors, ideas and institutions.[25] Bourdieu's field theory and his understanding of 'the state' as 'meta-field' framework, where certain fields (or actors engaged in fields such as the educational field, the cultural field, the economic field) battle to triumph over competing fields and over fractions within their field, resonates well in this context.[26] The EU, in particular, can also be understood as a state-like meta-field,[27] with distinct actors operating in specific settings with specific internalized norms and

22 See Deruityer (n 19) 110.

23 On the relevant case law of the Court of Justice of the European Union regarding the binding nature of soft law in the EU, see Petra Lea Láncos, 'A Hard Core Under the Soft Shell: How Binding Is Union Soft Law for Member States?' (2018) 24(4) European Public Law 755–784. See also more general Oana Andreea Ştefan, 'European Union Soft Law: New Developments Concerning the Divide Between Legally Binding Force and Legal Effects' (2012) 75(5) Modern L Rev 879; Gustaaf M Borchardt and Karel C Wellens, 'Soft Law in European Community Law' (1989) 14(5) Eur L Rev; Linda Senden, *Soft Law in European Community Law* (Hart 2004); Linda Senden, 'Soft Law and Its Implications for Institutional Balance in the EC' (2005) 1(2) Utrecht L Rev.

24 For a brief discussion, see Deruityer (n 19) 112-115. See also the studies referenced in the nn *below*.

25 See Mark Rhinard, 'Public Police Approaches and the study of European Union Justice and Home Affairs' in Ariadna Ripoll Servent and Florian Trauner (eds), *Routledge Handbook of Justice and Home Affairs Research* (Routledge 2018) 41-55.

26 See Bourdieu (n 1) 311: 'These fields are thus in competition with one another, and it was by and large in this competition that the state was invented, a kind of 'meta-field' power that was embodied by the king so long as there was a king, but which subsequently became the state. Each of these fields seeks to act on the meta-field, to triumph both over other fields and within its own field. This is abstract, but you will see very concretely, when I tell you the historical sequence, that the model works very well. What is constituted is thus a differentiated space of power, which I call the field of power (…) that is, a differentiated space within which the holders of different powers struggle for their power to be the legitimate one. One of the issues at stake in struggles within the field of power is power over the state as meta-power able to act on different fields (…) I could give examples. There is one very simple one, which is the retirement age. A change in retirement age affects every field: obtaining a universal reduction in the retirement age, for example, on one of the ways of regulating the struggles within each cam: 'Make room for the young!', 'War on the gerontocracy!'.' See on the relevance of Bourdieu and of sociological institutionalism for understanding data protection law, Julien Jeandeboz, 'EU Home Affairs and Technology' in Servent and Trauner (n 25) 180-190, in particular 184-185.

27 About the EU and its state-like attributes, see Jeremy Richardson, *European Union: Power and Policy Making* (Routledge 1996).

rules that guide their behaviour and thinking ('habitus'). We therefore welcome recent contributions in literature that contain in-depth studies of the individual EU related actors within specific fields of policy.[28]

But the analysis should go beyond established institutional boundaries. Is the European Commission, for instance, only *one* actor? If formally speaking it should be considered so, it remains a puzzling actor that does not exist in the constitutional landscape of Member States usually characterised by three powers (legislative, executive and judicial). The Commission blends features of both the legislative and executive power. Well-known for its agenda setting role with regard to regulation, its role in policy-making is much broader and complemented by a phletora of agencies, such as the Joint Research Centre (JRC) and the European Union Agency for Network and Information Security (ENISA).[29] They too are formally speaking 'the Commission'. But even within the confinements of its legal task, there is much confusion about the multifaceted role of the Commission as a regulator within *and* outside the EU. In both spheres, it can best be understood as an early shooter of ideas, a player that sets agendas and whose ideas function as the main reference points in the regulatory follow-up to these agendas.[30]

In our view, the Commission can hardly be understood as a homogenous body but qualifies in several respects as an autonomous policy hub with specific rules, actors and tensions.[31] Battles and competition between Commissioners, Commission departments and agencies determine who speaks on behalf of the Commission. One would only have partial knowledge of classical EU data protection law, without understanding the rule-making role of DG JUST, the EDPB or the EDPS. Similarly, one would only partly comprehend the role and background of recent EU Big Data related laws discussed *below* without seeing the reduced rule-making role of DG JUST and the lower impact of the expert advice of the EDPS and the EDPB, since these 'new' laws are coming from other (sub)fields within the Commission (such as Directorate-General for Communications Networks, Content and Technology (DG CNECT) or Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW)).

III. Framing and Facilitating Big Data within the Data Protection Canon (First Approach)

Let us now return to the question that triggered this contribution: *What is the message about Big Data in the recent basic European data protection documents coming from the EU and the CoE?* We already observed, that one cannot help being surprised by the apparent missed *rendez-vous* between data protection law and Big Data technologies. The concept is absent as such in the GDPR. There are very few obvious signs that Big Data challenges have been a major concern while drafting recent data protection documents. In spirit and in detail these can better be understood along the lines of the past data protection *acquis*: they consolidate, rather than transform EU data protection law.

This brings us to a first possible explanation: timing. The EU data protection reform was prepared

28 See, for example, the chapters on the Justice and Home Affairs-policies of the European Parliament by Ariadna Ripoll Servent, of the European Court of Justice by Ester Herlin-Karnell, of the European Commission by Natascha Zaun, of the Council and European Council by Christof Roos and of the national parliaments by Angela Tacea in Servent and Trauner (n 25). On the role of elite law firms in shaping European data protection law, see Nadezhda Purtova, 'Who Decides on the Future of Data Protection? Role of Law Firms in Shaping European Data Protection Regime', (International Review of Law, Computers and Technology 2013, vol. 28, issue. 2) 204-221.

29 See for instance: Joint Research Centre of the European Commission report on AI <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/artificial-intelligence-european-perspective> accessed 18 June 2019.

30 For example, on the international forum, on November 9, 2018, the European Commission submitted comments to the U.S. Department of Commerce's National Telecommunications and Information Administration in response to its request for public comments on developing the administration's approach to consumer privacy. See Hunton Andrews Kurth LLP, 'EU Commission Responds to NTIA Request for Comment on Developing the Administration's Approach to Consumer Privacy' <https://www.huntonprivacyblog.com/2018/11/13/eu-commission-responds-ntia-request-comment-developing-administrations-approach-consumer-privacy> accessed 18 June 2019.

31 On the under-researched role of the Commission, that is not as the Parliament or Council a co-legislator with concrete powers in the legislative process, see Natascha Zaun, 'The European Commission in Justice and Home Affairs: pushing hard to be a motor of integration' in Servent and Trauner (n 25) 409-420. The Commission is often described as a neutral and technocratic actor in the governance landscape of the EU, and observers break their head about whether the Commission is on the individual freedom side of the landscape or on the side of vested state interest (eg security). Zaun suggests that the Commission is best seen as 'an opportunistic actor' when it comes to normative positions, but also highlights the stable presence of a more-EU integration approach when possible and also stable variations in normative positions depending on the policy area at stake. See Zaun (n 31) 415.

around 2010, first drafts were made public in 2012[32] and the whole project was finalised in 2016.[33] The CoE reform was put on hold during this process and re-activated shortly after the adoption of the EU rules. This calendar of affairs should be combined with the phenomenon that most regulatory interventions are backward-looking. Reform in law is usually addressing issues that 'played' at the moment that reform plans were yeasting, but not necessarily those that 'play' when the reform is accomplished. There is some evidence for this hypothesis.[34] The term Big Data is vaguely defined and partly a buzz word which came into popular use only recently.[35] Therefore, it started appearing relatively late in EU policy documents. As a term it is absent, not only in the GDPR, but also in major EU statements on the Digital Agenda,[36] on cloud computing[37] or related documents from 2010 and 2012. It only appeared in the relevant policy documents of 2013 and 2014.[38] These texts, essential to understand the context of the recent data protection reform, bear witness of an ongoing but not yet fully matured learning process of the EU institutions concerning the economic and social impact of technological developments.

The second possible explanation is the GDPR's desire to be the law fit for the digital age, a piece of legislation that can remain in force for the next two decades at least. In its insistence to remain technologically neutral[39] the GDPR had to remain hesitant about specifically addressing Big Data. Its creators did not intent to reopen the legislative negotiations and develop specific rules every time a new technology emerges on the market.

Of course there were other factors, like lack of creativity in law making and evolving insight: there were simply no decent new innovative regulatory ideas regarding Big Data around at the time of the reform. Law was simply not ready for changing the rules of this technology game. Although in the years of reform there were some voices, especially from industry and from some US based academics,[40] arguing that data protection principles were outdated by the new technological realities (and suggested as an alternative risk-based and other 'new' approaches), the institutional voices were not willing to go ahead and defended the view that data protection principles could still be applied in a context of Big Data. For some, Big Data analytics were simply unacceptable and irreconcilable with European fundamental rights standards ('There is no need for special rules designed for Big Data because we do not want it at all'). For others, the matter was not that crystal clear and therefore pragmatism was the best approach: Big Data should be treated as any other processing of personal data and the rules developed in data protection legislation were seen as sufficiently regulating it.

The Article 29 Working Party ((WP29) the predecessor of the EDPB) - was at the forefront in this campaign. In the crucial reform years of 2013 and 2014, it released a number of policy documents on Big Data,[41] arguing several things at once: Big Data is nothing new, so no change is needed; Big Data has not

32 The Commission proposals for the GDPR and the LED were presented in the beginning of 2012.

33 The GDPR and the LED were adopted on 27 April 2016.

34 Hans Lammerant and Paul De Hert, 'Visions of Technology: Big Data Lessons Understood by EU Policy Makers in their Review of the Legal Frameworks on Intellectual Property Rights, Access to and Re-use of PSI and the Protection of Personal Data' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current developments in ICT and Privacy/Data Protection* (Springer 2016) 163-194.

35 On the distinction between established and emerging technologies, see Mohanad Halaweh, 'Emerging Technology: What is it?' (2013) 8(3) J Technol Manag Innov 108-115.

36 European Commission, *A Digital Agenda for Europe* (2010) COM(2010)245; European Commission, *The Digital Agenda for Europe – Driving European growth digitally* (2012) COM(2012)784.

37 European Commission, *Unleashing the Potential of Cloud Computing in Europe* (2012) COM(2012) 529.

38 European Commission, *Towards a thriving data-driven economy* (2014) COM(2014) 442; European Commission, *Report on the Implementation of the Communication 'Unleashing the Potential of Cloud Computing in Europe' Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Towards a thriving data-driven economy'* (2014) SWD/2014/0214.

39 GDPR, recital 15, first sentence: 'In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.'

40 Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Nw J Tech and Intell Prop 239; Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (NYU School of Law, Public Law Research Paper no 12, 2013) 56; Lokke Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' (Tilburg University, 2014).

41 eg WP29, 'Opinion 03/2013 on Purpose limitation'; WP29, 'Opinion 05/2014 on Anonymisation techniques'; WP29, 'Opinion 6/2014 on Legitimate interests'; WP29, 'Opinion 01/2014 on the Application of necessity and proportionality concepts and data protection within the law enforcement sector'; WP29, 'Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks' (30 May 2014); WP29, 'Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU' (16 September 2014).

achieved the promised results in terms of economy, security or science; even when Big Data delivers this does not mean that Europe with its fundamental right approach has to lower the protection of privacy given by the data protection framework and future developments *might* require innovative thinking on how some of the key data protection principles are applied in practice. The following quote gives a flavour of the general campaign:

> The Working Party acknowledges that the challenges of Big Data might require innovative thinking on how some of these and other key data protection principles are applied in practice. However, at this stage, it has no reason to believe that the EU data protection principles, as they are currently enshrined in Directive 95/46/EC, are no longer valid and appropriate for the development of Big Data, subject to further improvements to make them more effective in practice. It also needs to be clear that the rules and principles are applicable to all processing operations, starting with collection in order to ensure a high level of data protection.[42]

This campaign against making Big Data an explicit regulatory target was overall successful. The principles in both the EU and the CoE reform texts were simply restated as they existed (for instance, purpose specification/limitation and the compatibility test for further processing use still prevail), with only minor, but not unimportant Big Data-friendly amendments. We count at least three Big Data facilitators. Firstly, the general flexibility in the Directive 95/46/EC[43] with respect to further processing of personal data for historical, scientific and statistical purposes is maintained and enhanced in the GDPR. Already before the GDPR, the exception served as a legal basis for data mining by commercial entities and the development of group profiles.[44] Secondly, not truly an amendment but rather a clarification in the recitals, there is a reasonable test proposed to determine what personal data is.[45] Thirdly, there is Article 6(4) GDPR where criteria are given to assess the compatibility of the secondary use, including the flexible criterion of 'the existence of appropriate safeguards', understood equally as a soft enabling provision of Big Data practices.[46]

Convention 108+ follows a similar approach as the GDPR. For example, the principle of purpose limitation and permitted further processing are defined in the same way. More importantly, Convention 108+ adds a new Article 10 (Additional obligations), embedding at least four additional data protection concepts potentially open to Big Data processing – the principle of accountability, the data protection/privacy impact assessments, data protection by design and the risk-based approach. In order to prepare the ground for Convention 108+, its Consultative Committee (T-PD) issued, already in January 2017, the Guidelines on data protection in a world of Big Data.[47] The central message of these guidelines is that basic data protection principles and Big Data processing can exist in a symbiosis, if the controllers take the responsibility on their shoulders and at the same time follow the same steps as in the GDPR – data protection should be built in the early stages of the design of the processing; the controller should carry out an initial risk assessment; should follow up with

42 ibid WP29, 'Statement of the WP29 on the impact of the development of big data' 2.

43 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

44 Joris van Hoboken, 'From collection to use in privacy regulation? A forward-looking comparison of European and US frameworks for personal data processing' in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 231-257, 235-236.

45 GDPR, recital 26: '… To determine whether a natural person is identifiable, account should be taken of *all the means reasonably likely to be used*, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.'

46 GDPR, art 6.4: '… the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (f) the existence of appropriate safeguards, which may include encryption or pseudonymisation.'

47 Council of Europe, Consultative Committee of Convention 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* [2017] T-PD(2017)01.

a proper risk management policy and concrete efforts to minimise the risks; and should carry out a privacy impact assessment, if it is likely that the processing will affect the rights and fundamental freedoms of data subjects, etc.

This (first) strategy - upholding and enriching the principles while opening up to Big Data mechanics - has met with appreciation in literature,[48] nurturing some optimism about the ability of data protection law to uphold elementary Western values in the Big Data era,[49] especially taking into account the regulatory role played by national data protection authorities at the domestic level,[50] the EDPS and the EDPB at the EU level, and the role of experts and soft law recommendations at the CoE level.[51]

This optimism finds an unexpected bedfellow amongst deconstructivist authors that plunge deeper into the data protection edifice and find very little hard substance. The veil of principles draped around the data protection architecture conceals the absence of a precise framing power, harmony and continuity. A closer look at these principles reveals much discretion for experimentation with new technologies and business models.[52] Not all authors go as far as to claim that data protection is the door to permissionless innovation[53] and uncontrolled Big Data processing, but all agree that the data protection principles can endorse Big Data practices, because of their diluted or pragmatic nature.

One such author is van Hoboken who argues against critics like Koops that the data minimisation principle was never designed to prevent the development of massive databases or Big Data.[54] Von Grafenstein equally refuses to believe that European data protection law can and must be an obstacle to innovation processes such as Big Data. On the contrary, he argues that data protection law is a relatively modern regulatory approach suitable for regulating the often unforeseeable risks of data-driven innovation processes. This is in particular because of the purpose limitation principle, that when applied and interpreted properly, gives innovative data processors sufficient scope for implementation.[55]

IV. Facilitating Big Data Outside the Data Protection Realm: Six Examples (Second Approach)

Due to the position of influential stakeholders, data protection rules are often perceived as hindrance to innovation and development of new technologies.[56] It would, therefore, be unwise to proclaim a triumph of the European data protection community over pro-Big Data interest groups. Europe did not suddenly turn into a data protection fundamentalist region, suspicious of new opportunities. In fact, some commentators have observed that the GDPR has been un-

48 See, amongst others, Forgó, Hänold and Schütze (n 2) 17-42; Viktor Mayer-Schönberger and Yann Padova, 'Regime change? Enabling big data through Europe's new data protection regulation' (2016) 17 Columbia Sci Technol Law Rev 315–335.

49 See in particular Forgó, Hänold and Schütze (n 2) 35-40: controlled big data processing is possible under the GDPR, uncontrolled big data processing not.

50 See for example, the French DPA (CNIL)'s first analysis of the GDPR and Blockchain from November 2018 <https://aphaia.co.uk/en/2018/10/26/gdpr-blockchain/> accessed on 18 June 2019.

51 See for example, Council of Europe, Committee of Ministers (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010) and WP29, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, (3 October 2017) WP251.

52 See Paul De Hert, 'The Future of Privacy. Addressing Singularities to Identify Bright-Line Rules That Speak to Us' (2016) 2(4) EDPL 461-466 and Paul De Hert, 'Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection' (2017) 2(2) EDPL 2017 160-179.

53 See Adam Thierer, *Permissionless Innovation. The Continuing Case for Comprehensive Technological Freedom* (Mercatus Center at George Mason University 2016).

54 Van Hoboken (n 44) 237: 'Thus, the general (…) regime for the processing of personal data can best be characterized as 'yes, you can collect and process personal data as long as.' In sum, we may have to answer Koops's remarks about data minimisation cited in the intro- duction with the conclusion that the current European model was never designed to prevent the 'development of massive databases or the advent of the Big Data era. It merely aimed to put some reasonable conditions on the collection and processing of personal data, including that they are collected for acceptable purposes. This does not mean that there is no data minimisation principle. It just means that this principle does not stand in the way of legally permissible large- scale personal data processing activities'. A closer look at European practice reveals that these big data processing activities are tolerated as long as the controller identifies a wide series of purposes in advance or obtains consent for certain broadly formulated purposes.

55 Maximilian von Grafenstein, *The principle of purpose limitation in data protection laws. The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation* (Nomos 2018). See also the useful interview with von Grafenstein in the context of the book launch on <https://www.hiig.de/en/the-principle-of-purpose-limitation-in-data-protection-laws/> accessed 18 June 2019.

56 For example, see the opinion of Daniel Castro and Elaine Chivot that GDPR needs to be reformed if the EU would like to develop Artificial intelligence <https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/> accessed 18 June 2019.

dermined as the single and uniform set of rules for data protection across Europe due to inconsistencies in sectoral laws regulating the use of data[57]. Obviously, a *choose your battlefield* strategy was applied to foster more 'data-friendly' implementations of data protection.[58] Governments all over the world are actively thinking about new legislation, partly because current laws are seen as hindering technological innovation.[59] The announcement 'without data, we will not make the most of artificial intelligence, high-performance computing, and other technological advances'[60] illustrates the caution towards such a data-protection-fundamentalist approach.

Before discussing the measures addressing the abovementioned concerns, we observe that we are dealing *not* with DG JUST and *not* with the GDPR, but with *other* actors within the Commission propagating *other* measures. Now what are these 'other measures', mostly steered by DG CNECT and/or DG GROW, where the EDPS and the EDPB have a much smaller voice?

1. Data-Driven Economy and Directive (EU) 2019/770 (on Digital Content)

The European Commission presented an updated version of its vision on the data economy in its 2014 Communication *on a data-driven economy*.[61] The text presents data protection as an important tool to build consumer trust, but also announces that after the adoption of the GDPR and other EU reform texts, the Commission would work on guidance concerning Big Data-related problems such as data anonymisation and pseudonymisation, as well as data minimisation. Significant is a Briefing note on the proposal for the Digital Content Directive by the European Parliamentary Research Service.[62] The Briefing note is a Big Data hurrah but hints that one issue remains to be solved in the trilogue meetings, ie *the relationship between the Directive and EU public-law rules on the protection of personal data.* Amongst the many enthusiastic institutional and non-institutional stakeholders discussed in the summary is the EDPS. A closer look reveals that the objections of the EDPS are substantial - no hurrah but tangible objections against the EU initiative.[63] The EDPS was particularly critical of the basic idea laid out in the proposal of treating personal data as an object of contractual counter-performance ('paying by data' instead of by money). Because of the fundamental rights nature of personal data, it cannot be monetised. The EDPS was also very critical of the regulatory strategy and stressed that, as the legal requirements for processing personal data are laid down in the GDPR, this issue should not be addressed by legislation in the field of contract law. In the EDPS' view, the proposal overlaps with the GDPR and adopting it in its original form would lead to inconsistencies. The final text of the Directive even recognizes the potential conflict between some of its provisions with the rules of the GDPR and the ePrivacy Directive, by conceding to the prevalence of the latter.[64] Recital 24 of the Directive explicitly states that 'personal data is not a commodity', but the text then goes on to accept data as counter-performance for services.

Furthermore, and despite the opposition of the traditional data protection actors like the EDPS, data monetisation was more explicitly confirmed in recital 16 of the European Electronic Communications Code Directive[65], which stipulates that 'the concept of remuneration should therefore encompass

57 See the White Paper of Centre for Information Policy Leadership, 'GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges' (31 May 2019) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf> accessed 18 June 2019.

58 See on this strategy, Lammerant and De Hert (n 34) 186.

59 van der Sloot and van Schendel (n 2) 123.

60 'Andrus Ansip, Digital Single Market' <https://ec.europa.eu/commission/commissioners/2014-2019/ansip_en> accessed 18 June 2019.

61 European Commission, *Towards a thriving data-driven economy* (2014) COM(2014) 442.

62 European Parliamentary Research Service, Contracts for the supply of digital content and digital services, *Briefing EU Legislation in Progress* (February 2018), with a discussion of the European Commission's proposal for a directive regulating the private-law aspects of contracts for the supply of digital content and digital services in the internal market, COM(2015)634.

63 European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' (14 March 2017). See also European Parliamentary Research Service ibid 5.

64 See art 3(8) of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1. On the problematic relationship between this Directive and the GDPR, see more in Romain Robert and Lara Smith, 'The proposal for a Directive on Digital Content: A complex relationship with data protection law'(L ERA Forum 19, 2018) 159 <https://doi.org/10.1007/s12027-018-0506-7> accessed 18 June 2019.

65 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36.

situations where the provider of a service requests and the end-user knowingly provides personal data', or 'the concept of remuneration should therefore also encompass situations in which the end-user is exposed to advertisements as a condition for gaining access to the service, or situations in which the service provider monetizes personal data it has collected'.

2. Directive (EU) 2019/790 (Copyright Directive)

A second illustration is taken from the discussions about big data needs for available data and intellectual property rights that came to the fore in the context of the elaboration of the Copyright Directive and its Article 3, which the Commission conceived as an exception for TDM (text and data mining) for the purpose of research, including Big Data.

The Parliament's amendments[66] to the Copyright Directive[67] adopted on 12 September 2018 confirmed the European Commission's proposal to extend the scope of copyright to many publicly available datasets and to keep the exception in Article 3 limited. This choice was contested by the TDM community, including the academic community, who saw the exception as too narrow. For instance, the League of European Universities (LERU) argued that the Commission text should be improved and that the mandatory exception for TDM should be expanded to anyone having legal access to the content, and not only to research organisations for the purposes of scientific research.[68] However, the Parliament did not do much to change the Commission's version of Article 3. It sought to compensate by adding Article 3(a), allowing Member States and publishers to create further exceptions and to decide whether they would allow TDM beyond research organisations. Yet, this new exception was optional and will inevitably lead to fragmentation in EU, to the huge disappointment of the Secretary-General of LERU.[69]

Even though this Directive was recently adopted[70] and the final text of Article 3(a) (now Article 4) is much more to LERU's liking, we use this example in order to demonstrate a big data discussion, this time in the context of intellectual property rights, where the data protection community[71] was mostly absent or side-lined from a discussion with strong fundamental rights dimensions.

3. Open Data and Directive (EU) 2019/1024 (Re-Use of Public Sector Information)

A third illustration of Big Data targeting EU law regards the regulation of open data. We wrote in our introduction that Big Data should not be seen as an isolated phenomenon, but as being linked to other technical, social and legal developments and concepts. This explains why, for example, many Big Data initiatives are linked to open data and the idea that (government) data should be placed in the public domain.[72] The EU framework for this opening of data in the databases of governments was enshrined in Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information[73] (PSI Directive). On 22 January 2019, the co-legislators agreed on the new 'Open Data' Directive,[74] that entered into force on 16 July 2019. The new Directive addresses some of the

66 Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market (14 September 2016) COM(2016) 593 final <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0337+0+DOC+XML+V0//EN> accessed 18 June 2019.

67 ibid.

68 'The EP rightly decides to further discuss copyright' (LERU, 9 July 2018) <https://www.leru.org/news/the-ep-rightly-decides-to-further-discuss-copyright> accessed 18 June 2019.

69 On 12 September 2018, Kurt Deketelaere, SG of LERU, tweeted: 'it is really disappointing how the plenary EP today disregards the 21st century way of doing research where the right to read is the right to mine'.

70 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), PE/51/2019/REV/1 [2019] OJ L 130/92.

71 On 3 July 2018, the EDPS issued formal Comments only on art 13 of the proposed Directive regarding filtering obligations for platforms to avoid intellectual property infringements. See <https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-proposal-directive-copyright_en> accessed 18 June 2019. There was no general data protection discussion of the full proposal.

72 van der Sloot and van Schendel (n 2) 114. Traditionally, Open Data has been linked to efforts to increase transparency in the public sector and give more control over government power to media and/or citizens.

73 Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information [2003] OJ L 345/90, which entered into force on 31 December 2003. It was revised by Directive 2013/37/EU of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information [2013] OJ L 175/1, which entered into force on 17 July 2013. The political agreement to recast this Directive was reached on 22 January 2019.

74 Directive (EU) 2019/1024 (n 10). See also <http://europa.eu/rapid/press-release_IP-19-525_en.htm> accessed 18 June 2019.

issues mentioned in its evaluation report,[75] partly to accommodate Big Data developments. The objectives of this reform are the increase of the supply of high-value public data for re-use, limits to the use of exceptions to the principle of charging the marginal cost, and more real-time access to dynamic data via adequate technical means.

The Open Data Directive acknowledges the existence of the GDPR and the risk of placing personal data in the public domain. It therefore proposes a primacy principle of data protection stating that any PSI law has to be applied in coherence with data protection law and cannot create exceptions, as the protection of personal data is recognised as a fundamental right. In practice, this means that EU member states and PSI re-users must consider the principles and obligations of data protection law when applying or implementing the Directive. However, this does not imply that PSI that contains personal data cannot be opened; it rather demands a thorough assessment under which conditions the opening is lawful. In order to support the opening of PSI while protecting personal data, the Directive establishes such an (triple) assessment grid.[76] What we see is a fine example of using the GDPR as a reference point, while at the same time using specific laws to open up the GDPR protection in the name of Big Data. Note that the initiative has been thoroughly scrutinised by the EDPS in its Opinion 5/2018. Several of its recommendations were followed in the final draft.

4. Free Flow of Non-Personal Data and Regulation (EU) 2018/1807 (Framework for Free Flow)

A fourth illustration is the EU Regulation on the free flow of non-personal data.[77] The objective of this Regulation is to incite cross-border data flows across Europe in order to boost the development of artificial intelligence and supercomputers. The idea behind the Regulation is to unlock the potential of unstructured data sets for Big Data analysts across the EU and to put an end to certain national, regional or local requirements to locate data in a specific territory, even though the classical data protection actor, the EDPS, expressed serious criticism about it once again. The EDPS complained about the negative definition of non-personal data, which is likely to be very difficult to apply in practice, since the definition of personal data is broad and context-dependent. Moreover, the EDPS argued that the Regulation would automatically create a tension with the GDPR and would result in legal uncertainty as to which legal framework should apply in a given situation. [78]

5. Directive (EU) 2015/2366 (PSD2 Directive on Payment Services)

Fifthly, the Directive (EU) 2015/2366 on payment services in the internal market[79] (PSD2) is obliging banks transmit customer account information to other companies, provided that customers explicitly give their consent. The PSD2, which was supposed to be transposed into the national laws of the Member States by 13 January 2018, is seen as a 'gift' to fintech companies and as an assault to privacy, since the consumer will be pressured to give consent.[80] Bart Jacobs, Professor of computer security at Radboud University, senses 'a blind belief in everything that is called innovation and offers freedom of choice' behind the PSD2, but expects that this supposedly consumer-friendly law will ultimately weaken consumers' position towards ICT giants like Google. 'In practice, everyone just clicks 'agree' to be able to continue on a website or app and the grip on our data by tech giants such as Google and Apple will only ex-

75 Evaluation report (European Commission) on the Directive 2003/98/EC on the re-use of public sector information (25 April 2018) SWD (2018), 42; cf also Proposal (European Commission) for a revision of the Directive 2003/98/EC on the re-use of public sector information (25 April 2018) COM(2018), 1.

76 For a short discussion, see 'The PSI Directive and GDPR' (European Data Portal, 18 July 2018) <https://www.europeandataportal.eu/en/highlights/psi-directive-and-gdpr> accessed 18 June 2019.

77 Regulation (EU) 2018/1807 (n 11). See also <http://europa.eu/rapid/press-release_STATEMENT-18-6001_en.htm> accessed 18 June 2019.

78 EDPS, 'Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union' (2018) <https://edps.europa.eu/sites/edp/files/publication/18-06-08_formal_comments_freeflow_non_personal_data_en.pdf> accessed 18 June 2019.

79 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) [2015] OJ L 337/35.

80 Bram Logger and Parcival Weijnen, 'De nieuwe Wehkamp. PSD2 – Brussel gooit onze bankgegevens te grabbel' *De Groene Amsterdammer* (5 december 2018, n° 49) <https://www.groene.nl/artikel/de-nieuwe-wehkamp> accessed 18 June 2019.

pand'. Interesting is the position of Sophie in't Veld, MEP and one of the framers in the European Parliament of the GDPR and very active when it comes to PSD2. This eminent privacy advocate sees no harm in the modernised banking solutions:

> PSD2 regulates an open market in the financial sector, so that handy apps such as AFAS Personal can be added. For privacy, we have the GDPR. Suppose you want such a housekeeping book: then you give permission to use your data exclusively for that housekeeping book. According to the GDPR, the company cannot do anything with it. And it is always your own choice whether you share information.[81]

On the other hand, from the correspondence between Sophie in't Veld and the EDPB, it is obvious that she has major concerns with some of the basic data protection requirements in the interplay between the GDPR and the PSD2, such as the choice of the legal basis, the so-called silent party data and the PSD2 notion of explicit consent, which appears to be different from the notion of explicit consent in the GDPR[82]. We note that MEP in't Veld asked a series of questions to the EDPS, the EDPB and the Commission, while only the replies of the EDPB attracted a lot of attention. This development is interesting since it highlights the importance of the new voice in the EU fora. In the future, we will have to assess whether the EDPB will act systematically on such matter or only when it is called upon, whether the EDPS will refrain from action when the EDPB takes the lead, and whether EDPS and EDPB will act jointly more and more, like in their recent joint opinions on the eHealth Digital Service Infrastructure[83] or the US Cloud Act[84].

6. The Artificial Intelligence Ethics Guidelines (8 April 2019)

Finally, we observe the work of different EU actors on the development of Artificial Intelligence (AI) and the related policies. In June 2018, the Commission established a High Level Expert Group on Artificial Intelligence (HLEG)[85], composed of 52 expert representatives from academia, civil society, as well as industry. In his work Bourdieu put a lot of emphasis on the phenomenon of expert commissions and comities. Often they serve as good illustrations of how states and their agents function. Questions such as 'who sets up a commission?', 'when?' and 'who selects the members?' are central in his investigations. We think Bourdieu would have appreciated some spotlight on the High Level Expert Group on Artificial Intelligence. In its first year of operation, the HLEG issued Ethics Guidelines (8 April 2019)[86], which do not address the compliance of AI with the existing regulatory framework. The Guidelines instead focus on developing the principles and requirements of ethical Artificial Intelligence, as an additional condition for accomplishing Trustworthy Artificial Intelligence. According to the Guidelines, that goal may be reached only if Artificial Intelligence is both lawful and ethical. To that end, the HLEG proposed four basic ethical principles: Respect for human autonomy, Prevention of harm, Fairness and Explicability. From those principles, they derive seven practical requirements for the trustworthy Artificial Intelligence: Human agency and oversight, Technical robustness and safety, Privacy and data governance, Transparency, Diversity, Non-discrimination and fairness, Societal and environmental well-being and Accountability.

On its end, the Commission did not simply endorse these guidelines. Instead it decided to accompany the publication of the guidelines with its own Communication 'Building Trust in Human-Centred Artificial Intelligence'[87]. While the Commission 'welcomes the work of the AI high-level expert group and

81 Quoted in Logger and Weijnen ibid.

82 EDPB, Letter to MEP Sophie in't Veld (5 July 2018) <https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf> accessed 18 June 2019.

83 EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI) (10 July 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_201901_ehdsi_0.pdf> accessed 16 July 2019.

84 EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (10 July 2019) <https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en> accessed 16 July 2019.

85 'High-Level Expert Group on Artificial Intelligence' <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence> accessed 18 June 2019.

86 'Building trust in human-centric AI' <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top> accessed 18 June 2019.

87 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *building trust in human-centric artificial intelligence* [2019] COM (2019) 168 final.

considers it valuable input for its policy-making'[88], it emphasises that 'many existing (and often use- or domain-specific) provisions of Union law of course already reflect one or several of these key requirements, for example safety, personal data protection, privacy or environmental protection rules.'[89] The Communication explicitly mentions the 'GDPR, the Free Flow of Non-Personal Data Regulation, the Cybersecurity Act and the proposal for the new ePrivacy Regulation as a strong regulatory framework that will set the global standard for human-centric AI.'[90] The Commission is therefore protective about the EU *acquis* (as it should be), by pointing out that a lot of the elements for Trustworthy Artificial Intelligence are hard legal obligations of the operators, and not, as the HLEG Guidelines might be understood, principles which *could* be implemented in order to mitigate ethical concerns. In the years to come, the Bourdieuan grid will be paramount for understanding the different interpretations to what extent Artificial Intelligence is (not) already regulated and how much more regulation we (do not) need, both within the Commission and in a broader EU institutional arena.

V. Regulatory Failure or Painful Postponement of the Real Regulatory Exercise? (Conclusion)

In this contribution we looked at the interaction of laws and Big Data technology. We discussed data protection, for the simple reason that if personal data is processed, Big Data providers have to comply; and although Big Data is sometimes about non-personal data, it is more often *about* or *accompanied by* personal data. We focused on European data protection law, governed within the EU by the GDPR and other relevant texts, and within the CoE by Convention 108+ and its soft law instruments.

We observed that most of these instruments recall the general data protection principles but hesitate to go into the details about the processing done by contemporary private and public actors. Big Data relevant processing practices (web crawling, data mining, data matching, etc) are simply ignored by the EU data protection reform and the CoE Convention and soft law instruments.

This analysis is not written in a tone of alarm. Things could have been addressed more explicitly, but due to the flexibility of its principles, data protection law has always something to say, even when a technology or practice is not called by name. [91] So behind the silence, there is a strategy. This strategy was supported for years by many stakeholders and explains why the EU and the CoE reform texts are what they are ('silent on Big Data').

However, we have demonstrated that times have changed and that many Big Data-friendly legislative initiatives have been implemented in recent years either through soft law or through regulation drafted outside the field of data protection law (second strategy). Key policy makers, like MEP Sophie in't Veld, see in principle no problem with this strategy: 'for privacy there is the GDPR, and for having your bank data collected by non-banking actors there is the PSD2. The complete picture is obtained by reading both instruments together'.

True as this might be, there is an evident risk of losing the 'holistic balance'. These 'small' and mostly sectorial Big Data initiatives go about it in their own way and do not place the data protection legislation in the centre of the debate.[92] The GDPR and Convention 108+ do not have a special place in these Big Data friendly instruments and their usual spokespersons, the EDPS and the EDPB, are constantly forced to appear in new regulatory contexts without the familiar rules and actors. We saw how the EDPS in the context of the Digital Content Directive and the European Electronic Communications Code got marginalised by the presence of many other institutional and non-institutional expert and societal groups. Both EDPS and the EDPB will, therefore, - in a regulatory landscape characterised by scale (or 'field') pluralism - have to reconsider their strategy.

88 ibid 4.

89 ibid 3.

90 ibid 2.

91 For some, the reform texts *are* Big Data friendly or at least Big Data liberal because their silence creates a void that is promptly filled in by pro-Big Data players. Cf Maria Eduarda Gonçalves, 'The EU Data Protection Reform and the Challenges of the Big Data. Remaining uncertainties and ways forward' (2017) 26(2) Information and Communications Law 1; Purtova (n 28) 220.

92 On the regulatory approach of the EU, regulatory law rather than coherency law, see Roger Brownsword, *Law, Technology and Society: Reimagining the Regulatory Environment* (Routledge 2019) 341. The author nicely explains why experience teaches us that the EU is not keen on integrating novel laws in their context (the coherency approach), but almost always regulates from scratch having only little attention for existing (domestic and European laws).

Moreover, the classical method of voicing their point of view (through Opinions commenting on legislative developments) does not work in the case of the creation of ethical expert groups on algorithms, and is rarely used to react to soft law moves such as recommendations by the Commission to ensure open access to research data, and guidelines to foster data-sharing between companies.

The problem seems less urgent in the case of the GDPR and Convention 108+. With their broad scope one would not expect detailed provisions (on top of the many provisions that are there now) and modest optimism about a principle-based approach can be defended. However, here too there is a regulatory challenge. All kinds of actors outside the classical data protection field are laying the foundations for a European Big Data friendly architecture. Our brief discussion of the European Commission Communication *on a data-driven economy* and the Digital Content Directive; the Copyright Directive; the Open Data Directive on the re-use of public sector information, the 2018 EU Regulation on the free flow of non-personal data, the PSD2 Directive and the Artificial Intelligence Ethical Guidelines teach us that all kind of actors are making policies and their interests are most likely to prevail. A real conversation between Big Data and data protection seems to be avoided as much as possible.

In our past writings we have opposed the idea of data protection law as a homogenous bundle of values and principles and contrasted this with the understanding of this area of regulation as a series of laws (plural!), each being the outcome of specific power relationships, taking the form of different sets of principles, concrete subjective rights and rules.[93] Today we want to add a bit of Bourdieu to that characterisation, by highlighting that these laws are the outcome of struggles between agents or holders of different power that are using European organisations (for example, DG CNECT v DG JUST) and state decision-making machineries to impose their views on issues, such as, in this case, the relationship between Big Data practices and data protection principles. Agents (such as the scientists or industry) with a different capital (economic, social and cultural) and with different field-rules as compared to the actors that we know from the classical data protection field, might not have obtained a constraint-less playing field in the recent data protection reform products, be it at the level of the CoE or EU, but have triumphed in CoE soft law instruments and recent ad-hoc EU laws to obtain recognition as legitimisation of their views and interests. European data protection law is far from homogenous.[94] It is a fragmented policy field producing unpredictable outcomes partly due to the variety of institutions and institutional actors that are active on a plurality of subfields.

93 Paul De Hert, 'Data Protection as Bundles of Principles' (n 52) 160.

94 See Paul De Hert and Vagelis Papakonstantinou, 'Data protection policies in EU Justice and Home Affairs. A multi-layered and yet unexplored territory for legal research' in Servent and Trauner (n 25) 169. About the disjointed character of the field of cyber crime, see Helena Carrapico and Benjamin Farrand, 'Cyber crime as a fragmented policy field in the context of the Area of Freedom, Security and Justice' in Servent and Trauner (n 25)146.