BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 9 N° 1 OCTOBER 2023

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

POST-GDPR LAWMAKING IN THE DIGITAL DATA SOCIETY: MIMESIS WITHOUT INTEGRATION

Topological understandings of twisted boundary setting in EU data protection law

By Paul De Hert*

* The author wants to thank Cristina Cocito (FRC, VUBrussels), Andrés Chomczyk Penedo (LSTS, VUBrussels), Dimitra Markopoulou (LSTS, VUBrussels), Juraj Sajfert (LSTS, VUBrussels), George Bouchayar (LSTS; VUBrussels and University of Luxemburg), Taner Kuru (Tilburg University) and Dr. Richa Kumar (Trilateral). I would like to honor my collaboration with Vagelis Papakonstantinou (LSTS, VUBrussels) over the past years. Some of the ideas presented here are the result of our discussions and blogs. The author uses both singular ('I') and plural ('we') tenses. It came naturally and he hopes the readers will understand.

DISCLAIMER

The opinions expressed in this paper are those of the author/s.

Contents

1 Prelude: my past Paper on regulatory data protection approaches

In the past, I looked at the conspicuous absence of terms like 'big data' and 'data analytics' in the major data protection instruments that saw the light between 2016 and 2018 at the level of the European Union (EU) and the Council of Europe (CoE).1 Crucially, a Bourdieusian grid provided me with a theoretical lens to understand conflicts and collaborations between various agents that inhabit the various departments and agencies at the European level. In mapping the conflictual and collaborative elements of the (non)-regulation of these novel data-driven economy-phenomena, the study identified two regulatory approaches that were competing with each other in the drafting era, namely, 'taming the big data and other data driven phenomena with existing data protection legislations' or 'ignoring their presence when regulating data protection' and second, 'to address data driven practices and challenges in a more granular way at more regulatory frameworks other than the traditional data protection platforms'.

Europe's basic texts of data protection, namely, the EU General Data Protection Regulation (GDPR)[2] and the CoE Convention 108+,[3] illustrate the first 'hands off' approach: new data driven practices are not addressed specifically. The underlying feeling of these instruments is that classical data protection principles 'will do the job', a feeling supported by those agents and actors who are of the view that existing data protection law is sufficient.[4]

The second approach is of reformation outside the data protection legal canon where aspects of the data driven society are addressed in the most unlikely regulatory frameworks.[5].

---

[1] De Hert and Sajfert, 'Regulating Big Data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective', 5/3 *European Data Protection Law Review* (2019) 338.
[2] Regulation (EU) 2016/679, OJ 2016 L 119/1.
[3] Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 1981 ETS 108.
[4] By probing further into the view of 'sufficiency of existing data protection laws', the study highlights that in fact, these actors and agents are grappling with the enormity of the social and economic implications of Big Data resulting in the conspicuous absence of regulations on Big Data. This hesitation has resulted in addressing Big Data concerns on the side-lines and references to these can be found in Working Party 29, Directive 95/46/EC, Recital 26 GDPR, Article 6(4) GDPR and Article 10 Convention 108+.
[5] Using the lens of field, the study looks at the measures steered by EU departments such as DG CNECT and DG GROW where big data has been present. These include: 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, 2 July 2014, COM(2014) 442 final; Directive (EU) 2019/770 of 20 May 2019 concerning contracts for the supply of digital content and digital services, OJ 2019 L 136/1; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the

While mapping these two approaches and looking at a first set of EU-post GDPR laws, I brought to the fore the politics and power that shape the creation of laws and I was able to highlight both the heterogeneity of the EU and the CoE, and the differences between the two regional organizations.[6]

The complexity of the EU regulatory machinery is furthermore intensified by the particularities of the European Commission, at least from a traditional constitutionalist viewpoint. This strange heterogeneous body, 'shooter of ideas' and 'agenda setter', has key elements of legislature and executive blended in its role. Crucial here is to understand that the Commission consists of several departments (DG's or directorate generals) and is complemented by a range of agencies.[7] In order to grasp a complete picture of the emergence of the data protection regulatory framework, one needs to look at the whole of actors and agents, and their interest and motivations.[8] The state or in this case, the Commission, with its

---

Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ 2019 L 130/92; 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, OJ 2019 L 172/56; 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, OJ 2018 L 303/59; 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, OJ 2015 L 337/35, and High-Level Expert Group on Artificial Intelligence (AI HLEG), *Ethics Guidelines for Trustworthy AI* (2019), available at https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top (last visited 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, European Commission, *High-level expert group on artificial intelligence*, available at https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence (last visited 18 June 2019).

[6] I concluded that the EU should not be understood as an international organization like the Council of Europe, but as a state in itself (in the sense giving to it by Bourdieu in *On the State*). For instance, the creation of soft laws plays out differently at different level. At CoE level, one witnesses a definite hardening of soft laws. The ECtHR is an eminent CoE-body and it is organized such that a binding interpretation of one of the CoE recitals or CoE soft law instruments render it as a hardened, binding law. On the other hand, at EU level, the process of hardening of the soft law is not that visible. Further differences can be explained by elaborating of the different organizational and agential elements of these organizations. The CoE is organized as a classical international organization with a high impact role for agents whose meetings and collaborations are often defined by secrecy and confidentiality. In contrast to the CoE, the EU under the rubric of Lisbon Treaty has a more classical model of law making with the European Parliament representing the European demos, the Council representing the member states and the Commission which works as an initiator. Notwithstanding the constitutionalist structure defined by Lisbon, some secrecy at EU level 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.

[7] *See* the list of 56 Departments and Executive agencies of the Commission, European Commission, *Departments and executive agencies*, available at https://ec.europa.eu/info/departments_en (last visited 26 May 2021).

[8] Trying to understand policy making in the EU data protection sphere by looking only at Directorate-General JUST (Justice and Consumers), author of the GDPR, and by neglecting the respective agendas of Directorate-

institutions acts as 'organized fiduciary' and as a 'viewpoint on viewpoints, as Bourdieu coins it.[9]

2 About this paper. Preserving the boundaries of data protection law in post-GDPR laws

In this contribution I intend to push the research further while fully concentrating on EU developments. I look at a second set of post-GDPR laws, while preserving my initial questions about how the different regulatory actors involved in EU law consider the data protection principles as spelled out in the GDPR: *do they take these principles into account? only by lipreading or mimetics or is there a genuine effort to apply data protection? (substantive integration) If there is anything like an integrative effort, what form does it take: vague or precise (formal integration)? If so, what explains the EU approach and, eventually, how ought it change? How should they do it in my view?*

My approach is topological in the sense that I am interested in understanding how the boundaries and other properties (read 'rules and principles') of data protection law are preserved under the continuous regulatory deformations (applying, stretching, twisting, crumpling, and bending) through the multiple post-GDPR laws. My main finding is that boundaries and properties are not always well preserved in the process of continuous law making of the digital data society. Integration, denial or mimetics? (See on these terms *below*). That is the theme of this contribution. All post-GDPR laws, - four in total-, are discussed in terms of background and their data protection deformations. For lack of space, more concrete analysis of specific legal provisions in the EU laws discussed is not provided for, although it would make the argument stronger. Our first case study (on the cybersecurity

Generals such as CONNECT (Communications Networks, Content and Technology), COMP (Competition), ENER (Energy), FISMA (Financial Stability, Financial Services and Capital Markets Union), GROW (Internal Market, Industry, Entrepreneurship and SMEs), HOME (Migration and Home Affairs), Directorate-General, MOVE (Mobility and Transport), RTD (Research and Innovation) and other directorates and agencies is too narrow. When European banks find difficulties with Facebook's project to start producing its own payment system (implying a lot of personal data processing), they go to DG FISMA and not to DG JUST. If there are data protection problems with the Directive (EU) 2015/2366 of Payment Services (n. 6), it is because DG FISMA was the fiduciary and not DG JUST who proposed the GDPR. Similar story for stakeholders regarding automated cars, health, and drones … all go to their respective platforms.

[9] P. Bourdieu, On the State. Lectures at the Collège de France 1989-1992, (2012), at 23-44.

directive) will be a bit more extensive to suggest the analytical approach and structure to follow in a longer study.

We open with an example of *ex-during* or *eodem tempore*[10]-GDPR law making in the EU, in this case NIS or Cybersecurity Directive (section 3).[11] Then follow three shorter *ex-post* studies: the EU regulations on drones (section 4), the proposed Data Governance Act (DGA) (section 5),[12] and the AI Ethical Aspects Resolution and (proposed) Regulation (section 6).[13] In each section, I will look at the explicit connections with the GDPR. At the same time, these short descriptions also allow us to capture how regulators are addressing contemporary data-driven practices more explicitly in this era of the post-GDPR drafting.

The case study descriptions are rather flat. The more critical analysis of these case studies, bringing to the fore their salience for the general theme of this contribution, is reserved for section 7. We do not discuss all post-GDPR digital society related laws for lack of space, but the scheme of analysis proposed can be used for analyzing them. We will refer to laws that are not object of a case study here where necessary (such as the the DSA[14] and the DMA[15]).

Are all these initiatives the result of harmony and coordination with the GDPR rules and principles or rather of conflicts and deviations? In section 7, I introduce the theme of *GDPR mimesis* that, in my view, enriches the denial/integration discussion. On the Internet *mimesis* is characterized as a term in literary criticism and philosophy that carries a wide range of meanings, including imitation, non-sensuous similarity, receptivity, representation, mimicry, the act of expression, the act of resembling, and the presentation of the self.[16] *Mimicry* is the act, practice, or art of mimicking and in biology stands for the resemblance of one organism to another or to an object in its surroundings for concealment and protection from predators.[17] I like the biological definition of *mimicry* and, in general, the element of ridiculing

[10] Note that there is no Latin 'ex-' word for this category.
[11] The analysis is somewhat detailed to introduce the core theme of this study (integration).
[12] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final.
[13] EP Resolution of 20 October 2020, Framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).
[14] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 852 final.
[15] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final.
[16] Wikipedia, *Mimesis*, available at https://en.wikipedia.org/wiki/Mimesis (last visited 26 May 2021).
[17] The Free Dictionary, *Mimicries*, available at https://www.thefreedictionary.com/mimicries (last visited 26 May 2021).

suggested by the term, but I will use for communicative purposes the more neutral term *mimesis*. Together with Papakonstantinou, I distinguish between three forms: definitional, substantive, and symbolic mimesis.[18] These terms will be further clarified with illustrations taken from our findings on the DGA (section 5). Problems with mimesis are identified in section 7 with a strong insistence on the value of integration that has been often neglected in the laws that I discussed.

Subsequent sections will, relying on law in context-literature, formulate several alternative explanations for the current twisted landscape of data protection law making in Europe (section 8 and following). I will discuss the specific nature of EU regulation as a first factor (section 8), then focus on the regulatory reality of mixing laws and regulations with other regulatory instruments (section 9) but also on the all too human phenomenon of lack of creative thinking of regulators when confronted with new developments (section 10).

The explanations offered in these sections will furnish us with a more realistic understanding of regulatory change, which is not the same as bland acceptance of the outcomes. This study is opposed to *mimicry*, prudent with *mimesis* and in favor of careful *integration* of legal rules in a pre-existing framework of GDPR principles and rules. Only then, boundaries of data protection law will be able to function properly. The study concludes by advancing a perspective on regulatory change in EU law-making (section 11).

3 NIS Directive: Common Objective, No Integration (Case Study 1/*Eodem Tempore*)

3.1 Background

As early as 2009, the EU Commission, under the direction of two different DGs, the DG Connect and the DG Just, begun its consultation on the legislative process that eventually led to the adoption of the NIS Directive[19] and the GDPR. As regards the Directive, in 2009the

[18] Papakonstantinou and De Hert, *Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI*, (1 April 2021) European Law Blog, available at https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/ (last visited 26 May 2021).
[19] Directive (EU) 2016/1148, OJ 2016 L 194/1. *See* Markopoulou, Papakonstantinou, and De Hert, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation', 35/6 *Computer Law & Security Review* (2019) 105336.

Commission published its *Communication on the protection of critical information infrastructure against large scale cyber-attacks and disruptions*. A more concrete approach was adopted with the Commission's Proposal for a Directive, which was released in 2013. From 2013 to 2015 the Commission, the Council and the Parliament discussed intensely the draft put forward by the Commission and these discussions resulted in the NIS Directive, that entered into force in July 2016. The deadline for national transposition by the EU member states was 9 May 2018.

We briefly recall the chronological facts about the birth of the GDPR in a footnote,[20] to highlight the progression in parallel of the two law-making processes. Yet, the two processes happened completely independently. This is depicted in their texts as they hardly acknowledge one another.[21]

The reasons behind this detached approach while negotiating the two documents, that are, at least by appearances, related,[22] may only be assumed.[23] There is no doubt that the two documents should have been better aligned and integrated. Not so much because of their scope, aim, or purpose,[24] but because of practical reasons: it is possible and frequent that

[20] The GDPR, replacing the first EU data protection law (Directive 95/46/EC, OJ 1995 L 281) was the result of a long process as well, started in 2009, through a relevant public consultation launched by the Commission. This was followed by a Communication released by the Commission in 2010. After receiving comments from all major participants in the process, this stage was concluded in 2012 with the publication by the Commission of the first draft on a Regulation. Due to significant delay by the Council, the process was finalized three years later, in December 2015. The Regulation was published in April 2016 with effect from 25 May 2018.

[21] In particular, the NIS Directive refers to processing of personal data in its Article 2, where it is stated that '*processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC*'. A very generic reference let alone outdated, given that the GDPR was already published. Reference to personal data in the context of NIS is also made where cooperation with data protection authorities when addressing incidents resulting in personal data breaches is regulated (Article 15 para. 4). From its part, the GDPR takes account of cybersecurity-related processing, only for its own aims and purposes, for example when clarifying that '*processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security constitutes a legitimate interest of the data controller concerned*', also listing CERTs and CSIRTs among recipients of these clarifications (Preamble 49).

[22] Both have very similar provisions that impose adopting security measures and policies, adopting security breach notification, setting up supervisory authorities and foresee in a sanction mechanism.

[23] Whether this approach was the right one is a question that cannot be answered easily. As far as the 'why' is concerned, what instantly comes in mind, is the practical dimension of the question. Two processes run in parallel, by separate DGs, under different responsible teams, each of which had its own agenda. Also, at the Council, different Groups worked on each text in parallel but never interacted.

[24] In the GDPR it is personal data protection as a fundamental right in Article 16 Treaty on the Functioning of the European Union (TFEU). In the NIS Directive it is the security of networks. Consequently, the two documents do not have the same scope, aim or purposes.

network and information systems are used for the processing of personal data: Does this lead to the conclusion that both legal instruments find application at the same time? If yes, how?[25]

3.2 The Overlap Between the NIS Directive and the GDPR: more detail

To better understand the need for integration in the light of overlapping scope, we first need to examine the affected parties in both cases. GDPR applies to all undertakings that operate as data controllers or data processors, regardless of their nature or special features. The NIS Directive on the other hand applies only to operators of essential services (OES) and digital service providers (DSP). A possible overlap therefore would occur only if a hospital, for instance, as an OES, that is also a data controller, witnessed a security breach, which at the same time constituted a personal data breach. In other words, the Regulation does not cover security breaches that do not involve personal data violations, whereas the Directive does not affect undertakings that do not fall under these two categories (OES and DSP).

Once it is established that an undertaking operates under both capacities, the next question that needs to be answered is whether the security requirements imposed by the GDPR and the NIS Directive coincide, in the sense that an undertaking that falls under the scope of both instruments needs to apply all suggested security measures. *Should therefore the undertaking in question have an active cybersecurity policy and an active data protection policy even though they may overlap to some extent?* Answering this question is important in order to establish whether this undertaking is compliant under both regimes.

- Even in case some security measures are in practice identical, the security requirements imposed by the GDPR should not be confused with the ones imposed by the Directive.[26]

[25] In practice this question breaks down into the following sub-questions: Do affected organizations by the NIS Directive need to comply with security requirements imposed by the GDPR for the protection of personal data as well? In case a security breach in the context of the NIS Directive is also a personal data breach according to the GDPR, should the player involved apply the notification process described in the Directive or the one of the Regulation or both at the same time? In the above case, which authority should be responsible to handle the case? Finally, when it comes to penalties for a breach that is both a NIS security incident and a GDPR personal data violation should a cumulative penalty be imposed or alternatively one for each breach?

[26] The first target the data processing itself (Article 32 GDPR) and are designed to ensure the security of personal data, whereas the second include technical and organisational measures which intend to protect network and information systems against the risks posed to their security. Furthermore, the fact that a violation of an obligation under the Directive leads to a violation of an obligation under the Regulation does not automatically

- In the same context, notification of a security breach (NIS) should not be confused with that of a personal data breach (GDPR).[27] It is possible that an incident, even though leading to a personal data breach, is not fulfilling the conditions of notification taken from the Directive.[28]
- Finally, the issue of penalties should be addressed accordingly. There are different processes and obligations that are violated and therefore the penalties provided by the two instruments should add up.

In our view, in absence of case law and given the limited guidance found in the two legal instruments on this issue, the affected undertakings should comply with the requirements and processes indicated by both the GDPR and the NIS Directive. But that is too general and is not of a nature to hide coordination problems and concerns about whether, for example, double administrative sanctions can be issued for the same incident and whether security measures adopted under one regulatory tool (e.g., the GDPR) are sufficient to comply with the requirements stemming from the other one.[29]

Maria Grazia Porcedda has tilted this analysis to a higher level with her study of data breach notification-duties, that are incorporated not only in the NIS Directive and the GDPR but also in other cybersecurity (and data protection) related legislative instruments.[30] Porcedda

---

mean that that the violated right is the same or that the rule of law actually being breached is the same. To the contrary, the legal right protected under the two documents is completely different, the Regulation protects the individuals' rights against the violation of their personal data, whereas the Directive protects network and information systems against cyber incidents. Protection of individuals rights, including that of personal data, occurs only incidentally and is not the direct purpose of the NIS Directive.

[27] The first refers to the obligation of the undertaking to notify any incidents having a significant impact on the continuity of the service they provide (Article 14 NIS) whereas in the context of the GDPR this involves the notification of a personal data breach (Article 33 GDPR).

[28] The practical complications of choosing one process and one authority against the other cannot be analysed here.

[29] Comp. with the intervention of Zenzi De Graeve at the joint workshop on the EU cybersecurity law of 11 October 2019 organized by the Cyber and Data Security Lab (CDSL) and the Brussels Privacy Hub (BPH); *See* on her intervention Jasmontaitė-Zaniewicz, *Mapping EU cybersecurity law and its future challenges. Minutes of the CDSL & BPH EU Cybersecurity Law workshop*, (12 November 2019) available at https://cdsl.research.vub.be/en/minutes-of-the-cdsl-bph-eu-cybersecurity-law-workshop (last visited 26 May 2021).

[30] These include the e-Privacy Directive, Directive (EU) 2002/58, OJ 2002 L 201/37. This Directive has been amended by Directive (EU) 2006/24, OJ 2006 L 105/54 and Directive (EU) 2009/136, OJ 2009 L 337/11; the Framework Directive, Directive (EU) 2002/21, OJ 2002 L 108/33; the Electronic Identification and Assurance Services (eIDAS) Regulation, Regulation (EU) 910/2014, OJ 1999 L 257/73; and the PSD2, Directive (EU) 2015/2366, OJ 2015 L 337/35. In Porcedda, 'Patching the patchwork: appraising the EU regulatory framework on cyber security breaches', 34/5 *Computer Law & Security* (2018) 1077. Porcedda proposes to group all these internal market instruments into two regimes. The e-Privacy Directive and the GDPR concern breaches affecting personal data, 'data breaches' for short; the remaining instruments concern 'incidents' or 'breaches of security' or 'loss of integrity' or 'security incidents' which do not necessarily affect personal data.

observes that the definitions across these laws vary, but that they have a common final objective – the protection of information and its confidentiality, integrity, and availability.[31] We end by observing that the complications of a possible overlap between the two instruments were partially and broadly addressed in the Commission's proposal for the NIS Directive, but disregarded in the process that followed.[32] As far as the GDPR is concerned, no specific reference to the two documents' relationship is made.

4 Regulatory Strategy: Uniform Enforcement

4.1 Regulation (EU) 2018/1139 on common rules

Drones, unmanned aircraft systems (UAS) as industry and policy makers like to call them, are an interesting topic for understanding data protection and privacy discussions. They raise a lot of questions and beg for more detailed regulations.

The basic document is Regulation (EU) 2018/1139 *on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency*.[33] The regulation was published slightly after the entry into force of the GDPR on 22 August 2018 and aimed, *inter alia*, at creating a legal framework for the safe operations of drones in the EU by means of a risk-based approach. The preamble contains a vague reference to fundamental rights and makes some promises about future privacy safeguards to be introduced.[34] A closer look reveals that the Regulation does not do anything extra, beside making this announcement. Towards the

[31] Her final recommendation, to consider a unified law to address the issue information security and encourage the development of a mutual learning mechanism, is worth coming back to at the end of our study which I will do.

[32] In this first draft released by the Commission, it was suggested that in the cases where personal data were compromised as a result of incidents, member states should implement the obligation to notify security incidents in a way that minimizes the administrative burden in case the security incident is also a personal data breach in line with the Regulation. It was furthermore suggested that ENISA could assist by developing information exchange mechanisms and templates avoiding the need for two notification templates (Recital 31 of the Proposal for a Directive). The Proposal also addressed the issue of the sanctions and mentioned that member states should ensure that, when a security incident involves personal data, the sanctions foreseen should be consistent with the sanctions provided by the Regulation (Article 17 of the Proposal). Nevertheless, the final draft of the Directive included none of these thoughts and was limited to mention in its Article 15(4) that '*The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches*'.

[33] Regulation (EU) 2018/1139, OJ 2018 L 212/1.

[34] Preamble 31 Regulation (EU) 2018/1139: 'In view of the risks that unmanned aircraft can present for safety, privacy, protection of personal data, security or the environment, requirements should be laid down concerning the registration of unmanned aircraft and of operators of unmanned aircraft.'

end of the Regulation there is a provision that urges Member States to 'carry out their tasks under this Regulation' in accordance with the GDPR.[35] All other references in the text to GDPR are about pilot-data processing, not about protecting citizens against spying by drones.[36] In one of the Annex of the Regulation ('Annex IX Essential requirements for unmanned aircraft') there is a bit more: an interesting suggestion (para. 1(3)) to consider the principles of privacy and protection of personal data by design and by default, and a rule to register operators of unmanned aircraft in accordance with the implementing acts referred to in Article 57, where they operate drones that present risks to privacy, protection of personal data, security, or the environment (para. 4(2)(b)).

4.2 The 2019 Commission Implementing Regulation (EU) 2019/947 on rules and procedures

So far, the EU has come up with two relevant post-GDPR texts in this topic. First there is the Commission Delegated Regulation (EU) 2019/945 *of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems*.[37] This first regulation contains no data protection/privacy relevant provisions and no reference to the GDPR.

Better fairs data protection in the second instrument, the 2019 Commission Implementing Regulation 2019/947 *on the rules and procedures for the operation of unmanned aircraft*.[38]

---

[35] Article 132 Regulation (EU) 2018/1139: '(1) With regard to the processing of personal data within the framework of this Regulation, Member States shall carry out their tasks under this Regulation in accordance with the national laws, regulations or administrative provisions in accordance with Regulation (EU) 2016/679. (2) With regard to the processing of personal data within the framework of this Regulation, the Commission and the Agency shall carry out their tasks under this Regulation in accordance with Regulation (EC) No 45/2001.

[36] The Preamble 28 insists that 'the rules regarding unmanned aircraft should contribute to achieving compliance with relevant rights guaranteed under Union law, and in particular the right to respect for private and family life, set out in Article 7 of the Charter of Fundamental Rights of the European Union, and with the right to protection of personal data, set out in Article 8 of that Charter and in Article 16 TFEU, and regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council'. Interesting is a subsequent paragraph where a duty to register drones is announced.

[37] Commission Delegated Regulation (EU) 2019/945, C/2019/1821, OJ 2019 L 152/1. This 42-articles-long regulation contains a chapter on general provisions (chapter 1), followed by a chapter on UAS intended to be operated in the 'open' category (chapter 2) as opposed to drones operated in the 'certified' and 'specific' categories (chapter 3). In these chapters there are sections on product requirements, obligations of economic operators, conformity and notification of conformity assessment bodies and on Union market surveillance, control of products entering the Union market and Union safeguard procedure. Two last chapters deal with third country-UAS operators (chapter 4) and with final provisions (chapter 5).

[38] Commission Implementing Regulation (EU) 2019/947, C/2019/3824, OJ 2019 L 152/45.

This text has no chapters or sections, but simply list 23 articles and an annex.

The following data-related provisions are of interest:

- *Registration:* registration-duties are imposed on operators, whose drones have sensors capturing personal data, unless such aircrafts are deemed toys[39] within the meaning of Directive 2009/48/EC ('products designed or intended, whether or not exclusively, for use in play by children under 14 years of age').[40]
- *Responsibility:* Operators are to be held responsible for compliance with, among others, privacy requirements or measures protecting against unlawful interference and unauthorized access.[41] If required, they must undertake personal data protection impact assessments in accordance with the General Data Protection Regulation.[42]
- *Geographical zone-determination:* Member States may determine geographical zones for or 'safety, security, privacy or environmental reasons', and may among others, restrict or limit drone operations and access.[43]

In addition, there are two GDPR references.[44]

In none of the two instruments one finds a thorough integration of data protection principles as asked for by the GDPR and by Regulation (EU) 2018/1139.[45] Indeed, the above references to the GDPR do not necessarily enhance data protection. More attention could have been

[39] Article 14(5)(a)(ii) Commission Implementing Regulation (EU) 2019/947; Recital 16 Commission Implementing Regulation (EU) 2019/947.
[40] Article 2(1) Directive (EU) 2009/48, OJ 2019 L170/1.
[41] Article 1(a) Commission Implementing Regulation (EU) 2019/947 OJ 2019 L 152/45 Annex, Part B, UAS.SPEC.050.
[42] Article 1(a)(iv) Commission Implementing Regulation (EU) 2019/947, Annex, Part B, UAS.SPEC.050; Article 35 GDPR.
[43] Article 15(1) Commission Implementing Regulation (EU) 2019/947.
[44] A first reference to the GDPR in a footnote in Recital 19, suggesting that domestic registration systems comply with, among others, privacy and personal data related laws; and in the part of the Annex referring to responsibilities of operators, whose duty to establish procedures ensuring that all operations respect GDPR includes the requirement to carry out impact assessments. *See* Article 1(a)(iv) Commission Implementing Regulation (EU) 2019/947, Annex, Part B, UAS.SPEC.050.
[45] Regarding discussions prior to their adoption, according to the EASA's record, no GDPR-relevant debates took place. This could be because both instruments are delegated/implemented regulations; they do not follow the regular procedure; only technical issues are addressed by technicians/experts.

drawn, for instance, to technical data protection principles such as data protection by design.[46]

An additionally role could be played by the European Union Aviation Safety Agency (EASA). In its important 2019 Opinion (aimed at offering cost-efficient rules for low risk unmanned aircraft systems), the Agency regrettably does not refer to personal data protection.[47] However, it has proposed a draft annex to Implementing Regulation 2019/947 with two declarations: an '*Operational declaration*' and a '*Declaration of UAS operators that intend to provide practical skill training and assessment of remote pilots*'.[48] In the latter, drone operators would declare that personal data 'will be processed for the purposes of the performance, management and follow-up of the oversight activities according to Regulation (EU) 2019/947'.[49]

[46] This could be done in the Delegated Regulation (EU) 2019/945, whose subject matter is laying down the demands regarding design and manufacture. *However, the Delegated Regulation (EU) 2019/945 makes no reference to the GDPR and includes no data-relevant provisions.*

[47] EASA, *Opinion No 05/2019 on Standard scenarios for UAS operations in the 'specific' category* (2019), available at https://www.easa.europa.eu/sites/default/files/dfu/Opinion%20No%2005-2019.pdf (last visited 5 February 2020).

[48] EASA, Draft Annex to draft Commission Implementing Regulation (EU) .../... amending Commission Implementing Regulation (EU) 2019/947 as regards the adoption of standard scenarios (2019), available at https://www.easa.europa.eu/sites/default/files/dfu/Draft%20Annex%20to%20Draft%20Com%20Impl%20Reg%20%28EU%29%20...-...%20amending%20Reg%202019-947.pdf or https://www.easa.europa.eu/document-library/opinions/opinion-052019 (last visited 5 February 2020).

[49] This Opinion has not yet been officially published; and the text of the proposed Annex is available as a draft document (without date etc). It is noted that the 'Operational declaration' is mentioned explicitly in the text and Annex of the Implementing Regulation 2019/947, but it does not have a ready template (as the one provided by the above Opinion); nor does it explicitly refer to personal data. *See* Article 2 Commission Implementing Regulation (EU) 2019/947, Annex, Part B, UAS.SPEC.020: 'A declaration of UAS operators shall contain (a) administrative information about the UAS operator; (b) a statement that the operation satisfies the operational requirement set out in point (1) and a standard scenario as defined in Appendix 1 to the Annex; (c) the commitment of the UAS operator to comply with the relevant mitigation measures required for the safety of the operation, including the associated instructions for the operation, for the design of the unmanned aircraft and the competency of involved personnel. (d) confirmation by the UAS operator that an appropriate insurance cover will be in place for every flight made under the declaration, if required by Union or national law.'

5 Data Governance Act: Overlap, Obstinate Terminology (Case study 3/*Ex-post*-GDPR)

5.1 Background

Since late 2020, a new more ambitious post-GDPR legislation creation process that relates directly with the data-driven digital economy, as part of the European Data Strategy[50], has started. Most of the discussion on the matter so far has focused on the proposals titled as the Digital Services Act (DSA)[51] and the Digital Markets Act (DMA).[52] However, there is a third component to this new wave of regulatory initiatives from the European Commission that went by a bit under the radar.[53] In spite of this, it might be the single most important piece of the new set of law when it comes to regulating the data driven society and in particular the 'Big Data-aspects': the Data Governance Act (DGA) proposal.[54] Given its general applicability, it might provide some much necessary rules to address contemporary data practices in a comprehensive manner regardless if there are industry or sector specific rules.

As such, it is worthy to ask how does the DGA relate to the data-driven economic development that the European Commission is trying to foster? Together with the Open Data Directive, the DGA aims to encourage open data and the re-use of data. The main ambitions of the DGA are making public sector data further available beyond the Open Data Directive and to foster data sharing among businesses, against remuneration in any form. Also, the DGA tries to foster

[50] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, 19.02.2020, COM(2020) 66 final.
[51] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 852 final.
[52] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final.
[53] In this respect, certain civil society organizations, such as European Digital Rights (EDRi), have put this matter on the table and include the DGA in the overall analysis of the current policy discussion landscape about the future of the European digital economy. *See* EDRi, *EU alphabet soup of digital acts: DSA, DMA and DGA* (2020), available at https://edri.org/our-work/eu-alphabet-soup-of-digital-acts-dsa-dma-and-dga/ (last visited 5 March 2021).
[54] The European Data Strategy takes large data collection and data-analytics for granted, as it repetitively mentioned in that document, and as part of the data-driven economic future. A quick overview of both the DSA and the DMA proposals reveals to us that the data collection and exploitation by very large online platforms is a fact not questioned by neither proposal. In fact, it would seem the European Commission desire to expand who can benefit from data driven applications and allow small and medium enterprises to rely on such technological developments for the commercial and economic success. In this respect, those business models developed around these data intensive practices are not put under the spotlight and questioned but rather are acknowledged as a fundamental part of our digital economy and, consequently, regulated and integrated even further into our society by general application regulations in the whole EU.

data use on altruistic grounds and the use of personal data with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).

The opening remarks of its explanatory memorandum explicitly indicate that the purpose of the DGA is to support the sector-specific legislation[55] on data access, use, and re-use with a common background upon which those *lex specialis* on the matter can rest when in silence about certain issues or if they still haven't been adopted as European regulations, such as in the case of the financial services industry.

As for the content of the DGA, it has eight chapters, structured in the typical format of European regulations, starting with a chapter on definitions and scope. After that, it follows the subject matter of the DGA: (i) re-use of data held by public bodies; (ii) data sharing services; and (iii) data altruism. The remaining parts of the DGA tackle who are the competent authorities alongside the creation of the European Data Innovation Board as well as the granting of new powers to the Commission, much in a similar manner to what happens in the DSA and the DMA.[56]

5.2 Relation with GDPR: different definitions and open questions about consent

A burning question in common between all these proposals is how they related with the GDPR. Perhaps in the case of the DGA that question is even more pronounced as, in the words of the explanatory memorandum, '*[t]he instrument aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU*'. In this respect, the explanatory memorandum from the European Commission acknowledges that there is an interplay between the DGA proposal and the GDPR, which then confirmed in the wording used in the actual regulation proposal, such as Article 1(2).[57] The

[55] In this respect, the explanatory memorandum as well as the footnotes 26 through 38 in the Recitals of the proposed regulation point out to these sector-specific rules that should interact with the proposed DGA.
[56] This last matter, -the expansion of the powers of the European Commission-, shall be addressed later as it is possible to identify a clear change in the enforcement regime foreshadowed in these new proposals.
[57] Article 1(2) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act): '*This Regulation is without prejudice to* specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, *or requirements related to processing of personal* or non-personal *data*. Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional

question that could be raised in this respect is how this communion shall look like, in particular for two main reasons: (i) both pieces of legislation employ different terminology for the involved actors; and (ii) the scope of the DGA goes beyond what the GDPR has under its control. Therefore, the key area of discussion about the interplay between the envisaged DGA and the GDPR is how differences in definitions, in particular around three concepts: data[58], data holder[59] and data user,[60] have an impact on the application, the compliance, and the enforcement of both pieces of legislation.

The notion of 'data' as referenced in the current wording of the proposed DGA includes both non-personal and personal data.[61] The DGA would set a minimum set of duties and obligations for any data processing activity, regardless of this data being personal or non-personal. This approach provides a much-needed refresh to the debate around the (de)protection of non-personal data, since more and more of this kind of data can be grouped to arrive at personal data or, even more so, produce the same results on individuals without even setting a foot in the personal data realm.[62]

To achieve this, the DGA further departs from the traditional terminology employed in the data protection arena regarding the parties involved in the data processing activities. In this sense, the DGA talks about data holders and data users. From a data protection perspective, a data

technical, administrative, or organizational requirements, including through an authorization or certification regime, those provisions of that sector-specific Union legal act shall also apply.' (emphasis added)

[58] Article 2(1) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act): '…means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording'

[59] Article 2(5) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act): '…means a legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control'

[60] Article 2(6) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act): '…means a natural or legal person who has lawful access to certain personal or non-personal data and is authorized to use that data for commercial or non-commercial purposes'

[61] This is because the purpose of the DGA is to provide a default regulatory framework for information use, re-use and sharing, regardless of whether it is personal data or non-personal data. In this respect, the DGA can be applauded for acknowledging, even if it was not done on purpose, one of the most prominent debates around information and the border where it turns into personal data. *See* e.g., Bygrave and Tosoni, 'Article 4(1). Personal data' in C. Kuner, C. Docksey, and L.A. Bygrave (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (2020), at 103.

[62] In this respect, Purtova points out that the distinction between both regimes is pointless for an interconnected future populated by Big Data, IoT devices and intensive data-driven activities but instead the focus should be placed on providing legal protection in any scenario where an individual is involved and could be affected by harm. *See* Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', 10(1) *Law, Innovation and Technology* (2018) 40.

holder can be either a data controller or even a data subject; on the other hand, a data user can only refer to a data controller.

There are three main activities for which rules are provided in the DGA: re-use of public data; data sharing services; and data altruism. For this case study, focus shall be placed on the latter two newly created institutes by the DGA.[63]

Firstly, data sharing services. When it comes to data sharing services, the DGA stipulates that there are three activities covered in its provision: (a) intermediate between data holders and data users for the exchange of data through different means; (b) intermediate between data subjects and data users for the exchange of data through different means for the purpose of exercising data rights provided for in the GDPR, mainly right to portability; and (c) provide data cooperatives services, i.e. negotiate on behalf of data subjects and certain data holders terms and conditions for the processing of personal data. Article 11 provides for the conditions that must be met to provide any of these three services.

The DGA provides that the operation of a data sharing service must be notified to the competent authority in the relevant member state. When reviewing the wording used in the proposal text, it seems that the matter of an entity providing services in different jurisdictions is still under the same competent regulatory agency as it is provided for in the GDPR. As such, the question remains open as to whether this model would incur in the same problems as the GDPR.[64]

Secondly, data altruism. The other new relevant institute created for the data-driven era is the figure of data altruism, which is defined as '*…the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services*' (art. 2(10) DGA). It provides the possibility for data holders to make their data available for free or for a charge.

[63] The matter of re-use of public data needs to be read alongside the Open Data Directive, as well as the GDPR, and where much has already been written about.
[64] Following the same spirit as the GDPR, registration before a national authority is not necessary to begin operations but instead it would seem that the lack of notification could constitute an illegal provision of service. The notification must disclose a certain amount of information regarding the service itself, as noted by Article 10(5). Upon notification, the competent authority has a week to issue a standardized declaration; it is an open question if the data sharing service provider can effectively operate within that time window between the notification and the declaration.

This concept of data altruism allows to better understand the European Data Strategy envisaged by the European Commission, in particular when it comes to who,[65] and how one can make decisions regarding the use, re-use, and sharing of personal data. In this respect, consent plays a crucial role and the DGA proposal would seem to reject the application of any other legal basis for this kind of service. The question, as a consequence of selecting such a strict legal basis, is how the granularity demanded for having a legally valid consent can be achieved.[66] The GDPR has a very complex set of rules on consent, with variables such as age, use of sensitive information or not, and purpose of the processing. It is striking to see that the DGA fails to clarify how data altruism should work in practice in the light of these multiple consent formats in the GDPR. The DGA, as a legal framework that pretends to set up a framework on data altruism but that is silent on these complex matters, does not deliver its promises. We will come back to this 'failure' of the DGA in our section on mimesis (section 7 *below*).

6 EU Regulation of AI: Integration (Case Study 4/ *Ex-Post*-GDPR)

6.1 The AI Ethical Aspects Resolution from the European Parliament

Over the last few years, the European institutions have expressed their interest in strengthening the regulation of artificial intelligence technologies, addressing the call for a more transparent, robust, holistic, and coherent system for regulating the development and use of such technologies. This agenda is fuelled by the feeling that the GDPR and other laws in place remain sub-optimal on several fronts. It is not the place here to recall the history or the interplay between the different EU institutions with regard to AI policy making (from the

[65] When it comes to the entity that provides the data altruism services, Article 16 DGA states that it can only a non-for-profit legal entity and completely independent from any for-profit entity. In contrast to data sharing service providers, the DGA mandates the registration of data altruism organizations before national competent authorities. In a similar fashion, the entity needs to disclose certain information about its operations and the competent authority has a twelve week-period to grant the registration or deny it. Since the registration is necessary to provide the services, a data altruism organization cannot engage before such registration takes place.

[66] This is triggered because the wording used by the DGA would not be requiring such a detailed description of the purpose for which the data is envisaged to be used for.

Commission, over High-level expert group on artificial intelligence (AI HLEG) to the Parliament and back to the Commission), neither can we go in detail about the concrete proposals. Key here is to understand the priority given to aligning, applying, and improving the rules and principles of data protection law as found in the GDPR, or at least considering them.

In this sense, the AI Ethical Aspects Resolution from the European Parliament provides for a good example.[67] It suggests that the Commission introduces a Regulation 'on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies'. Read under a GDPR lens, the Parliament's recommendation essentially replicates the GDPR scheme (and follows closely even its structure). A new set of actors is introduced ('user', 'developer', and 'deployer', resembling GDPR's data subject, controller, and processor respectively) in Article 4. Its principles, outlined in Article 5, very much follow the GDPR's ones ('safety, transparency, and accountability'). Unmissable GDPR-reminding ideas include 'risk assessments' in Article 14 (Data protection impact assessments in the GDPR), 'compliance assessment' in Article 15 (prior consultations in the GDPR) or the 'European Certificate of Ethical Compliance' (European Data Protection Seal in the GDPR). In addition, the Parliament recommends establishment of 'national supervisory authorities' for monitoring all of the above (in Article 18); Space for a *European Data Protection Board* (EDPB)-like institution is openly left in Article 20.

6.2 The proposed 2021 Artificial Intelligence Act (AIA)

The main outcome of the mentioned interest in strengthening the current legal framework is the proposed Regulation laying down harmonised rules on artificial intelligence by the Commission, that is, the proposed 2021 Artificial Intelligence Act (AIA).[68] Let us just give one example of the interesting GDPR interaction taken from this ambitious piece of work. Interesting in comparison with the GDPR is how this Act defines the key participants across the AI value chain. Looking at the definitions in Article 3, we learn that *development phase* and

[67] Papakonstantinou and De Hert, *Refusing to award Legal Personality to AI: Why the European Parliament got it Wrong* (25 November 2020) European Law Blog, available at https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/ (last visited 26 May 2021).
[68] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, 2021.

use phase are the two main phases in the AI lifecycle, whose key participants are *providers*[69] and *users*[70] respectively. For our analysis it is relevant to note that the algorithmic issues and safeguards related to Article 22 GDPR only address the second stage of AI use.[71] The AIA proposal, on this important point, goes beyond the GDPR and states that already in the first stage of development appropriate human oversight measures should be identified and implemented by the provider (Recital 48):

(48) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role.

These duties for the providers are further elaborated in Articles 13, 14, 16, and 29 of the AIA text. Providers shall ensure high-risk AI systems are compliant with the human oversight requirement (art. 16(a) AIA). To comply with this requirement, they must design and develop AI systems in a way that they can be effectively overseen by human agents during the use stage (art. 14(1) AIA).[72] Before placing the AI system on the market, the providers either identify the appropriate measures to be implemented by the user, or identify and build them, when technically feasible into the system (art. 14(2) AIA). Such measures shall enable human agents -to whom human oversight is assigned- to understand the capacities and limitations

[69] Art. 3(2) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge.
[70] Art. 3(4) 'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity.
[71] The first *development*-stage is indeed out of the GDPR scope when it comes to providing governance mechanisms for automated decision-making, just as this important stage remained beyond the scope of legal scholars' analysis and policy solutions (Lehr and Ohm, 'Playing with the Data: What Legal Scholars Should Learn About Machine Learning' 51 *U.C. Davis Law Rev* (2017) 653, at 655). According to Almada, this is a narrow interpretation of the GDPR *that restricts intervention to the end stages would make it useless, but human intervention in the design stages may be more effective by proposing alternative models of the data that take such concerns into account* (Almada, Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems (2019), 17th International Conference on Artificial Intelligence and Law (ICAIL) 1, at 5).
[72] The Commission understands that the concept of human oversight focuses on the human agent interpreting and following or modifying the output at the use stage. This implies that 'oversight' as a requirement does not extend to concepts such as organizational oversight, although we can also qualify it as 'human' in a broad sense.

of the system, to correctly interpret its outputs, or to interrupt the system, among others, in the use stage (Article 14(4) AIA).[73]

To these duties to make AI-oversight possible, one need to add the transparency requirements laid down in Article 13 AIA,[74] and the obligations for users of high-risk AI systems anchored in Article 29 AIA. This last provision, in a nutshell, states that users shall utilize the information about human oversight measures to comply with their obligation to carry out a Data Protection Impact Assessment under Article 35 GDPR (art. 29(6) AIA).

Article 29 AIA shows a remarkable effort to bring the proposed regulation on AI into line with the GDPR.[75]

7 Mimesis, Consistency and Distinct Regulatory Objectives

7.1 The DGA as an example of GDPR mimesis

From the four case studies above, we identify in at least three of them an "ubiquitous" thread of mimesis with GDPR principles. In section 2, we contrasted *mimesis* as a more or less acceptable form of imitation, with *mimicry,* mockingly unacceptable imitation. But even mimesis in law can be controversial and, as shown *below*, can come at the expense of a lack of integration.[76] When looking at the previous sections, a light categorization of mimesis is

[73] Article 14(4): The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: *(a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible; (b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available; (d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system; (e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure*.

[74] These require that the oversight measures shall be facilitated to users in an accessible and comprehensible way (art. 13(2) and 13(3)(d)).

[75] This effort is often absent in other relevant recent EU laws. *See* Vagelis Papakonstantinou and De Hert, 'Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI' (1 April 2021) *European Law Blog*, at 3 via https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/. The following section draws heavily on this blog.

[76] The theme of *GDPR mimesis* serves to enrich our discourse and respond the question about how the EU considers GDPR principles and why it does so. The reason of this EU law making approach to technology are mapped out in the following sections to provide a realistic understanding of EU regulatory change.

possible on the following grounds: definitional mimesis, substantive mimesis, and symbolic mimesis. Let us illustrate this with our findings on the DGA (section 5 *above*).

Firstly, definitional mimesis. We saw that different terminology is introduced, in the form of 'data holders', 'data users', 'data', or 'data sharing' (Article 2 DGA). It looks like the GDPR but not exactly, since this text talks about 'data subjects' (meaning individuals), and 'controllers' and 'processors' (meaning those doing the processing) interact through 'processing' of common or 'sensitive' 'personal information' (meaning any operation on personal data) (Article 4 GDPR). Is this a problem? Perhaps, but the DGA is 1) focused on certain data actors (public actors, data sharing services, and data altruism entities:); 2) on certain activities regarding data (re-use of data held by public bodies and data sharing); and lastly 3) applies to all data, a notion that includes both non-personal and personal data (Article 2.1 DGA).

Then there is substantive mimesis in the DGA. Recall that the DGA identifies a special set of principles to govern the provision of data sharing services (Article 11 DGA), organizes a system of adequacy for data exports outside the EU (Article 30 DGA), and introduces new 'special' rights to assist individuals that want to engage in 'data altruism' (Article 19 DPA). Again, this should not be a problem. The GDPR can be seen as a basic set of rights and principles to protect personal data, but it can be justified in sectoral laws to advance the level of protection, like in this specific regulation that focuses on specific stakeholders and targets the sharing and use of personal and other data.

Finally, symbolic mimesis might be a more serious challenge. The DGA sets up a European Data Innovation Board that at a closer look is no more than an expert group advising the Commission to help regulating data sharing practices in Europe (Article 26 DGA). All useful, of course, but the name of this instrument simply suggests too much in the light of the legal powers and competences of *the European Data Protection Board* set up by the GDPR or the *Management Board of the EU Aviation Safety Agency* set up by Regulation 2018/1139 (discussed in our section on drones). Not everything can be called a 'board' at the price of confusing the citizen.

7.2 Ample GDPR Mimesis, Little GDPR Integration

Is GDPR mimesis unavoidable? Our discussion of the Drones Regulations showed a strategy of very loose and general references, but no application or real engagement with data

protection. That is questionable from an integration perspective (see *below*), but it can hardly be mimesis. Terms like lipreading and denial or avoidance seem more appropriate.

But the example of the NIS Directive (on network and information systems) discussed in section 3 shows that mimesis is not always applied. There are other, more recent examples. At the same time as releasing its DGA draft, in December 2020, the Commission also introduced two important proposals comprising the so-called Digital Services Act package:[77] the DSA[78] and the DMA.[79] Both texts are a counterexample of GDPR mimesis. Not a trace of the EU personal data protection scheme can be found in their texts. Why is that?

The DSA and the DMA, as was the case with the GDPR, are not designed from scratch. Particularly the DSA furthers and expands Directive 2000/31/EC *on certain legal aspects of information society services, in particular electronic commerce*.[80] This e-Commerce Directive is an impressive text by its own merit that, same as the 1995 Data Protection Directive, withstood for more than twenty years the internet revolution that took place in the meantime. In other words, the aim-setting of the DSA and the DMA is entirely different: they aim at regulating the provision of services over the internet. Their objective is to protect consumers and offer legal certainty to providers. They could well be the result of path dependency within the same policy cycle.

7.3 Is GDPR mimesis such a bad thing after all?

Does it not make sense for EU legislators to copy a model that has demonstrably served its purposes well, placing the EU at the international forefront when it comes to protecting individuals from the unwanted consequences of technology? Yes and no. From a legal-technical point of view, complexity is increased. If all the above initiatives come through, the same company could be 'controller' or 'processor' under the GDPR, 'data holder' under the DGA, and 'developer' under AI regulation – not to bring into the picture any DSA or DMA characterization. But perhaps ours is an age of complexity, and simplicity in the digital era is

[77] European Commission, *The Digital Services Act Package* (2021), available at: https://ec.europa.eu/digital-single-market/en/digital-services-act-package (last visited 26 May 2021).
[78] Digital Services Act (n. 52).
[79] Digital Markets Act (n. 53).
[80] Directive (EU) 2000/31, OJ 2000 L 178/1.

long foregone. Notwithstanding any such pessimistic ideology, the fact remains that lawyers and state authorities will most likely have a particularly hard time juggling simultaneously over all the above capacities. Consistency, if it ever was an EU law objective at all, as most pertinently questioned by Brownsword,[81] would be substantially hampered.

Perhaps then the GDPR has formulated an EU model for technology regulation? A kind of acquis? While perhaps tempting from an EU law point of view, in line with the 'Brussels effect' identified by Bradford,[82] this finding may prove problematic: would then the EU approach to technology essentially comprise a highly structuralist, bureaucratic approach composed of special roles, rights and principles and establishment of new state authorities?

Even under a straightforward, human creativity perspective, mimesis is a bad thing. One is allowed, and indeed compelled, to stand on the shoulders of giants but at some point, he or she must make his or her own contribution. Only then can they leave their mark. But in this we are not in creativity per se, but in law with its insistence on legal constraints, logic, and internal morality. Rules can be creative, but should be at least minimally clear and intelligible, free of contradictions, relatively constant, and possible to obey, amongst other things[83].

Perhaps the most salient aspect of post-GDPR lawmaking is its refusal to integrate the new in the old. We are not discussing different terminology here (see on that *above*), but coherence and substantive integration of old and new that should be spotlighted here. All post-GDPR laws state in their preamble that they are 'without prejudice to EU law and the GDPR in particular' or affirm 'in addition to their provisions, the GDPR provisions (also) need to be respected', but that does not bring us very far at all, on the contrary.

These disclaimers only make us more curious about how the GDPR and the post-GDPR laws integrate and interact concretely. That clarity is not given, even at the most elementary level. The GDPR requires for every processing a legal basis: any actor before processing personal data needs to identify a valid legal basis for that personal data processing activity and this can only be one the six legal bases for processing enumerated in Article 6 GDPR: consent; performance of a contract; legitimate interest; vital interest; legal requirement; public interest. One would expect from the DGA with its narrow scope (only three pillars or issues are dealt

[81] R. Brownsword, Law, Technology and Society: Reimagining the Regulatory Environment (2019) 155.
[82] A. Bradford, The Brussels effect: How the European Union rules the world (2020).
[83] L. Fuller, *The Morality of Law* (2nd ed., 1964).

with) to detail and further clarify what kind of legal GDPR-basis applies in these three specific contexts, but that does not happen. The only exception would be the third 'pillar' (data altruism) as the DGA is explicit: this activity should be based around consent and one cannot possibly rely on any possible other legal GDPR-basis. Then again, no more information is given, while the GDPR is very elaborated on the ingredients of valid consent (given by a clear affirmative act, freely given, specific, informed, unambiguous, revocable…), distinguishes between consenting to processing of normal data (Article 7 GDPR), consenting of sensitive data (Article 9 GDPR), consenting by minors (Article 8 GDPR), and add extra rules for international transfers of data. How does this play out in the context of data altruism (often involving very sensitive data such as health data)? One would have expected more clarificatory work in the DGA as a *lex specialis* to the GDPR, but in vain. A useful clarification could have been cross referencing with phrases like 'Consent in the meaning of Article 8 GDPR is needed….'.

Another example of unsatisfactory mimesis is the 2016 EU Police and Criminal Justice Data Protection Directive,[84] a 65-provisions-long text that was published the same day (4 May 2016) as the GDPR. The latter clearly served as a basis and starting point for most of the provisions of the Directive. The Directive faithfully adheres to all terms, principles (and most of the rules) from the GDPR but hesitates to go into the details about the processing work done by contemporary police and law enforcement. Big data relevant processing practices (web crawling, data mining, data matching, etc.) are simply ignored by the EU Directive. Moreover, ideas such as predictive policing are launched in the recitals and provisions of the Directive without any elaboration apart from the requirement that such processing operations need to be envisaged by law.

Let us now leave these case studies and return to our main inquiry: why is Europe missing its *rendez-vous* with the GDPR and its data protection principles and rules? Why is it producing data protection laws of a general nature and initiating data-driven focused reform via other, more recent, laws? How can we explain the lack of integration in the post-GDPR laws?

[84] *See* De Hert and Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive. A First Analysis', 7(1) *New Journal of European Criminal Law* (2016) 7.

8 Beliefs in Open Texture and Agencification (Factor 1)

8.1 The new regulatory state approach to address deficiencies in law making

The previous discussion with its insistence on careful integration of laws cannot be disregarded with a general account about generality of international legal instruments.[85] A more ambitious expectation about integration by international regulators is not unreasonable per se. Especially the EU legal apparatus seemed fit for the job of regulating at the European level in detail: the EU sought to replace diverse national laws mainly with *regulations*, single European-wide pieces of legislation, that harmonize national provisions, linked to cycles of revisions and procedural provisions that would update the legislation in question in the light of technical progress. The latest proposals, as shown in sections 5 and 6, would seem inclined towards this approach to ensure those objectives as much as possible.

However, some commentators call this expectation and approach to regulation (applied in many areas of EU law) an 'old approach' characterized by major deficiencies: time-consuming, involving time-lags (outdated at the moment of implementation), and lacking flexibility needed for changing consumer behavior and market innovation.[86] Like other international organizations, e.g. the Council of Europe, the EU was also confronted with another drawback of utilizing command-based techniques at the supranational level: it encountered more and more difficulties in achieving consensus in identifying collective policy goals and consensus in setting standards for achieving those goals.[87]

---

[85] So, we are not satisfied with a reminder about the limits of international or EU legal instruments and about the differences between EU regulations (the most centralizing of all instruments and are utilized to ensure uniformity) and directives (need transposition, and leave member states some discretion as to the form and methods used to transpose) and about conventions necessarily being vague. On this basis some would argue that silence on difficult integrative exercises or discretion is all that can be expected from international regulatory instruments, and we should bid farewell to our expectations and our trust in command and control via Strasburg or Brussels using *hard law* instruments such as regulations, conventions and directives and counting on domestic courts (and sometimes European Courts) to make it all work.

[86] 'It was considered time-consuming, given member-state sensitivities and decision-making rules that allowed for blockages, and it involved such a time-lag that by the time rules were adopted, they were already technically out of date. Other difficulties were that the regulations were too entrenched once passed, there was a degree of uniformity that reduced consumer choices and innovation, and the process made insufficient use of technical standardization and industrial norms—which led to duplications, delays, and inconsistencies' (R. Baldwin, M. Cave, and M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd ed., 2012) 392).

[87] 'As a result, supranational norms are often drafted in vague, aspirational or framework terms. Although these broad generalized statements of principle may conceal underlying political disagreement concerning their scope and content, they pose considerable difficulties for those responsible for their implementation. As domestic enforcement studies demonstrate, vague and indeterminate rules do not translate easily into hard, practical norms for guiding behaviour and identifying contraventions' (B. Morgan and K. Yeung, *An Introduction to Law and Regulation: Text and Materials* (2007) 323-4).

As a reaction, the EU became a 'new regulatory state' and did three interconnected things: it started to keep some of its hard laws rather open textured, -even in its regulations-; it relied for further guidance on the Court of Justice of the European Union (the Luxembourg Court endowed with more and more competences), *and* it relied on soft law and agency decision-making. This new approach has been in vogue since the 1980s and is an obvious explanatory factor for the lack of integration and the use of vagueness in post-GDPR laws.

8.2 Agencification and the reliance on expert systems in data protection law

In particular, the role and strategic use of agencies, present in all possible institutional shapes and seize, is remarkable.[88] Their role, next to court dispute resolutions systems, is crucial in view of the presence of supranational vague norms that conceal underlying political disagreement between states (see *above*). Legally binding court decisions might clarify these rules; but they may fail effectively to defuse underlying political disagreement and, therefore, call into question the legitimacy of these adjudicatory determinations.[89] This is where the agencies come in. As a network of expert actors operating on basis of the same generally applicable standards, they can succeed in establishing global epistemic communities in specific policy sectors (like data protection) with shared knowledge, culture, and values that overcome disparities in national conditions, values, and practices.[90]

The prominence of agencies in the data protection field and the reliance on their guidance and the guidance by the Court of Justice of the European Union (CJEU) can be highlighted with CJEU judgements such as *Patrick Breyer* and *ASNEF and FECEMD*, prohibiting states to

[88] R. Baldwin, M. Cave, and M. Lodge (n. 87) 397-8 with ref. to Thatcher and Coen, 'Reshaping European Regulatory Space' 31(4) *West European Politics* (2008) 806. 'The agency landscape has not stopped evolving and has taken different institutional shapes ranging from national regulators acting together, a mix of Commission and national regulatory staff, to purely "EU-level regulators" and the EU Commission acting as regulator'.
[89] B. Morgan and K. Yeung (n. 88), 323-4.
[90] Ibid. 324. with ref. to C. Joerges and E. Vos (eds), *EU Committees: Social Regulation, Law and Politics* (1999): 'These epistemic communities have considerable potential to transcend local allegiances, especially where the appearance of universalistic, objective foundations for expert knowledge opens the possibility of depoliticising the rule-making process. It is therefore hardly surprising that international networks of experts have proliferated at the supranational level, accompanied by optimistic accounts of their potential role in global governance'.

clarify European data protection via national laws and creating a guidance monopoly for the European Court and data protection agencies.[91]

In our view, a first plausible explanatory factor for lack of integration is a consequence of the European regulatory approach and machinery relying heavily on agency expert knowledge, the pro-Europe activism of the CJEU, and soft power. Traditional European law-making via regulation and directives is now steered at the more general, while the more concrete norm-building work and the more controversial or complex work is left over to less democratic decision-making,[92] either by the agencies acting together or by the CJEU.[93] This translates into exercises of simple mimesis in post-GDPR laws and their lack of substantial integration of data protection rules and principles.

9 Beliefs in a Broader Mix of Regulatory Instruments and Institutions (Factor 2)

9.1 The GDPR itself requires a broader mix of regulatory approaches

I discussed in the introduction (section 1) a first approach towards post-GDPR lawmaking, especially amongst the data protection authorities in the period 2012-2016 regarding Big Data ('let it come and prove itself, no reason to change the principles now')? This attitude is still there and will probably inspire future reactions, at least from the institutional actors in data protection law, to any allegations (like the one in this paper) about a missed regulatory *rendez-*

[91] De Hert, 'Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer', 3(1) *European Data Protection Law Review* (2017) 20 with a discussion of Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* (ECLI:EU:C:2016:779); Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD)* (ECLI:EU:C:2011:777). *See also* van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation', 4(4) *International Data Privacy Law* (2014) 307, at 319-20: 'By undermining the diversity in national approaches, the democratic legitimacy of the right to data protection may be undermined as well'.

[92] Compare 'by charging an agency with the implementation of a general regulatory mandate, legislators ... avoid or at least disguise their responsibility for the consequences of the decisions ultimately made' (*See* Fiorina, 'Legislative Choice of Regulatory Forms', 39 *Public Choice* (1982) 33, at 47. In 1986 a more refined delegation mechanism was identified: delegation to agencies is pursued in areas of high uncertainty, whereas a reliance on statute or enforcement through courts is pursued in case of certainty about the future. *See* Fiorina, 'Legislator Uncertainty, Legislative Control, and the Delegation of Legislative Power', 2 *Journal of Law, Economics and Organization* (1986) 33. *See* also R. Baldwin, M. Cave, and M. Lodge (n. 87) 56.

[93] The CoE machinery operates is a quite similar way, with treaties and conventions drafted in general terms, narrowed down in recommendations and other soft law guidance documents.

vous of the GDPR and the post-GDPR laws. To put it differently, one can probably expect a strong rejection by the data protection establishment of charges of under-regulation[94] and/or disconnection.[95] Some professionals from other circles (industry, academia) will join in[96], especially those that criticize the limits of the hard and traditional supranational law making (discussed in the previous section). *O, sancta simplicitas!*, they argue, traditional law making is so imperfect and slow and regulatory detail is overrated. A more superior understanding of regulatory strategies is needed with an awareness of the existence of alternative regulatory instruments to complement vague (or sometimes to detailed) supranational norms and principles.

Command and control (use of legal authority and the command of law to pursue policy objectives) is indeed only one option. Next to soft law, there is self-regulation and there are other modes of delegating the regulatory function to bodies beyond the state via controlled certification schemes and audits of corporate risk management systems.[97]

Those that accept open texture in hard laws and agencification (*see* previous section), will often insist on the available alternatives to laws in the narrow sense. They will point at the optimal mixes of regulatory instruments and institutions made possible in and demanded for by the GDPR itself. This text is indeed a meeting point of different regulatory strategies: there are not only the very general but over-inclusive principles (that will apply to all that is yet to come, even big data), but where possible there are detailed rules, whereas data subject rights are further expanded, the enforcement mechanism is strengthened, and controllers are

[94] On these charges, *see* R. Baldwin, M. Cave, and M. Lodge (n. 87) 69.
[95] On the concept of regulatory disconnection with regard to law and technology, *see* R. Brownsword and M. Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials (Law in Context)* (2012) 398 and foll.
[96] Sometimes it is without a good reason and the overall motor of critique is disbelief in regulatory interventions, disbelief in law. About 'futility', 'jeopardy', and 'perversity' as three rhetorical strategies commonly employed to resist progressive policy interventions, *see* R. Baldwin, M. Cave, and M. Lodge (n. 87) 73 with a discussion of the work of Albert Hirschman who identified these strategies.
[97] R. Baldwin, M. Cave, and M. Lodge (n. 87) 105 and foll.

entrusted with duties to better inform via treat and incentives.[98] Ideas such as certification, seals, and impact assessment are present and made possible by the GDPR.[99]

Open texture and detail, together, allow Europe to face new or specific data protection challenges and frame the data-driven economy without stifling it.[100] Post-GDPR laws should therefore be understood in a double perspective: standing on the shoulders of the GDPR they add some detail, but also some vaguer newer ideas. They can add vagueness to the vagueness/detail of the GDPR or add detail to the vagueness/detail. In its terminology, the DGA seems to add merely vagueness to the GDPR (section 5), but that would be an incomplete analysis. The stakeholder perspective (the Act contains specific chapters on (i) public bodies; (ii) data sharing services; and (iii) data altruism) is a valuable addition to the GDPR that is particularly weak in addressing actors by labeling them all 'controllers'. The Commission is enthusiastic and applauds this mix of regulatory instruments expanding GDPR protection (by including non-personal data) and clarifying GDPR protection (by voting laws on specific actors or problems). This approach would seem, according to the Commission, the way to foster data-driven innovations relying upon big data collection and data analytics.[101]

9.2 What to think of this 'enriched' approach?

When a better understanding of regulatory alternatives to detailed laws boils down to defending open textured norms and to adding vagueness rather than detail to data protection

[98] 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', 3(2) *European Data Protection Law Review* (2017) 160. *See also* De Hert *et al*., 'The proposed Regulation and the construction of a principles-driven system for individual data protection', 26(1&2) *Innovation: The European Journal of Social Science Research* (2013) 133. On law as threat and law as umpire, *see* B. Morgan and K. Yeung, (n. 88) 5-6. On the basic capacities, other than command and acting directly, of states (to deploy wealth to influence conduct: to harness markets and channel competitive forces to particular ends; to inform e.g. so as to empower consumers; to confer protected rights so as to create desired incentives and constraints: R. Baldwin, M. Cave, and M. Lodge (n. 87) 105-106.

[99] *See* Kamara and De Hert, 'Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a reformed landscape', in R. Rodrigues and V. Papakonstantinou (eds), *Privacy and Data Protection Seals*, *28 TMC Asser Press-Springer, Information Technology and Law Series* (2018) 7.

[100] G. Malgieri and P. De Hert, 'Making the most of new laws: reconciling big data innovation and personal data protection within and beyond the GDPR', in E. Degrave et al. (eds), *Law, Norms and Freedoms in Cyberspace - Droit, Norme et Libertés dans le Cybermonde: Liber Amicorum Yves Poullet* (2018) 525. *See equally* Forgó, Hänold, and Schütze, 'The Principle of Purpose Limitation and Big Data', in M. Corrales, M. Fenwick, and N. Forgó (eds), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation* (2017) 17.

[101] In this respect, the European Data Strategy takes the GDPR as the basis upon which further regulations can, and should, be enacted.

law, we need not to be too enthusiastic. It is hard for me to see a problem with more detail in data protection law. The choice of the GDPR to add very concrete rules and more elaborated rights to the basis set of data protection principles that go back to the 70s and 80s, is not without justification. More detailed rules pose less considerable difficulties for those responsible for their implementation (see section 10 *below*) and fulfill human rights requirements such as transparency and foreseeability.

For some however recent reform has gone beyond the optimal mix by adding too much detail. Often heard in many, mainly oral, discussions, is that current data protection laws (especially the GDPR) are too long currently. A return to shorter texts with only the principles and some amendments would make these laws more resilient.[102] In these discussions, one hears strong echoes of well-known criticism on command-and-control strategies. Apart from the critique that many laws are the result of 'capture', by interest groups and civil society organizations, there are the concerns about the limits of the reliance on legal rules of command-and-control strategies and its alleged propensity to produce too many *and* unnecessarily complex and inflexible rules, strangling either competition or civil liberties depending on the success of interest groups.[103]

9.3 Detailed laws irritate

A more sophisticated and more fundamental skeptical stand is one that relies on system theory thinkers such as Niklas Luhmann, Gunther Teubner, and Helmut Willke that perceive law, economy, politics, religion, sport, health, family as subsystems with own rationalities and insist on the problematic nature of the belief that legal norms can directly intervene in these other sphere.[104] Especially the lack of power of law to intrude in the economy has received a lot of attention. To 'arrive' in the economic subsystem' translation with a legal message is

[102] *See* van der Sloot (n. 92) 318-22.
[103] R. Baldwin, M. Cave, and M. Lodge (n. 87) 108-9.
[104] B. Morgan and K. Yeung, (n. 88) 69-74; R. Baldwin, M. Cave, and M. Lodge (n. 87) 62-3 with a short discussion of G. Teubner, *Dilemmas of Law in the Welfare State,* (1986); G. Teubner, *Law as an Autopoietic System*, (1993); Teubner, Nobles, and Schiff, 'The Autonomy of Law: An Introduction to Legal Autopoiesis' in D. Schiff and R. Nobles (eds), *Jurisprudence*, (2003) 897; Luhmann, 'Law as a Social System' 83(1&2) *Northwestern University Law Review* (1989), at 136; Willke, *Systemtheorie III: Steuerungstheorie*, (1995). *See also* Rottleuthner, 'Biological metaphors in legal thought', in G. Teubner (ed.) *Autopoietic Law: A New Approach to Law and Society* (1988) 97.

difficult and implies distortions and time delays. In that respect a shorter document with data protection principles might be more effective to tame big data economics.

Interesting is Teubner's insistence on *irritations*. Attempts to intervention in subsystems, even with translation, are not necessarily successful because of the resistance of these subsystems to 'code' that is not theirs. Transplanting law and regulation in non-legal subsystems is at best creating 'irritation effects'. Other less desirable outcomes, but highly plausible, are mutual indifference (law is seen as irrelevant to the other sub-system) or colonization (either of the subsystem taken over by law, or of law being 'over-socialized' by the other sub-system).[105]

It would take more space to think through this analysis, but here is a first take:

On the one hand, it is very clear from political statements by EU political leaders that instruments like the DSA and the DMA (discussed in section 7 *above*) and other recent instruments such as Regulation 2019/1150, also known as the Platform-to-Business Regulation or P2B Regulation,[106] have the explicit aim to intervene in the market. The latter Regulation, for instance, seeks to bring fairness and transparency for businesses operating in the platform economy. It provides online businesses with a new set of rights that is intended to mitigate power imbalances between them and platforms. It is too early to assess the effectiveness of this agenda of the Ursula Von der Leyen Commission that started working in December 2019. Irritations are to be expected, but skepticism is not at its place: apparently the reliance on principles in the years before 2019 has not worked.

On the other hand, some post-GDPR laws are clearly designed to neutralize possible GDPR irritations to certain sectors. Instruments like the drones' regulations (section 4 *above*) and the PSD2 that had no other intention to please a series of actors (like the tech companies) by opening bank data to non-banking actors.[107]

[105] *See* Teubner, 'Das regulatorische Trilemma. Zur Diskussion um postinstrumentale Rechtsmodelle', 13(1) *Quaderni Fiorentini per la Storia del pensiero giuridico moderno* (1984) 109; R. Baldwin, M. Cave, and M. Lodge (n. 87) 63.
[106] Regulation (EU) 2019/1150, OJ 2019 L 186/57.
[107] *See* our analysis, De Hert and Sajfert (n. 2) 345-6.

Wrapping up our second factor, in our view, the optimal mix of regulatory instruments and institutions can account for the lack of substantive integration of GDPR principles in post-GDPR law making.

10 Lack of Creative Legal Thinking about Data Protection Implications (Factor 3)

In this section I come back to the theme of rules and detail, that was already touched upon previously. As fundamental rights-trained lawyers, we are often amazed by the intensity of the *rules v. principles* discussion in legal and policy fora. It is almost a religious thing, especially the belief of some (most) in principles (abstract, non-eroded by private interests, rational, channeling to the public good), coupled to a certain disdain for rules (ordinary and vulgar, detailed, quickly outdated, replaceable, political, etc.). Like fundamental rights, principles can be bended, expanded, eroded, and replaced.[108] There is no fixed list, and their number is (also) prone to inflation. So, there is inflation of rights and principles, just like there is rule-inflation.[109] Mobilizing the Luhmans and Teubners of this world in favor of data protection laws without rules, mainly spelling out the principles and no more, lacks profound substantiation.

'New' rule-based devices, such as privacy impact assessments and privacy by design, might make translation, irritation, and proceduralization possible. More so, when they spell out bright-line rules regarding controversial matters ('the age of kids to go on the Internet is x or y') they might be able to settle and stop confusion generated by these controversies. We briefly recall that complexity is one Luhmann's other central themes, for whom reduction of complexity is one of the distinguishing features of (sub- or social-) systems.[110]

[108] *See* what happened to the principle of data minimization in the Directive (*see above*). On the broadening of some principles and the quasi elimination of others (e.g., the principle of transparency) in data protection law, *see* van der Sloot (n. 92) at 311-4. On domestic police laws disregarding the purpose-specification principle, *see* Cannataci and Bonnici, 'The end of the purpose-specification principle in data protection?', 24(1) *International Review of Law, Computers & Technology* (2010) 101.
[109] On 'regulatory ratchet', *see* chapter 7 in E. Bardach and R. Kagan, *Going by the Book: The Problem of Regulatory Unreasonableness* (1982). *See also* R. Baldwin, M. Cave, and M. Lodge (n. 87) 108-9: 'Regulatory rules tend to grow rather than recede because revisions of regulations are infrequent; work on new rules tends to drive out attention to old ones; and failure to carry out pruning leads the thickets of rules to grow ever more dense'.
[110] N. Luhmann, *Social Systems* (1995); Bednarz Jr., 'Complexity and Intersubjectivity: Towards the Theory of Niklas Luhmann', 7(1) *Human Studies* (1984) 55.

In past writings, I have therefore not hesitated to applaud the insertion of more and more concrete rules in data protection reform texts. Like principles, rules can pressure legislators to reduce discretions in favor of the 'rule of law'. Although some might regard this as an invitation to excessive production of rules,[111] we think foreseeability of state actions and (other) infringements of fundamental rights is a worthy cause.

Of course, rules must be devised with care. In the area of police and law enforcement powers this boils down to finding the right balance between due process requirements and efficiency concerns. In the area of data governance, following our focus on the DGA, this boils down to achieving transparency, accountability and participation in the governance of data, personal or not[112]. Baldwin *et al.* open their chapter on *Explaining Regulatory Failure* with the observation that 'at the broadest level, regulatory failure can be explained by insufficient resources and by epistemological limitations 'failures of imagination'.[113]

Part of the problem is indeed creativity. It takes creativity to understand the relation and interaction between regulatory modalities such as technology, markets, social norms, and laws. It takes creativity to understand a phenomenon such as data altruism and apparently it takes years to frame it. Profiling and machine learning might be other examples. Is Article 22 GDPR all we have to say about automated decisions and profiling? Is human intervention and the prohibition to use sensitive data provided for by this provision all that is needed to regulate profiling well?

Similar questions regarding the DGA: does it provide any new form of governance or is it just another patch to the flawed current business models based around advertising? Are the providers of data sharing service any different from what we already have? Can data altruism organizations provide an alternative for fostering responsible data sharing to enable big data innovations without all the negative traits that they are currently producing? The fact that the DGA escapes the constraints of the definitions provided for by the GDPR and acknowledges that non-personal data also plays a crucial role in the development of data-driven businesses should already be applauded for providing an alternative to explore and try new paths, in spite

[111] Bardach and R. Kagan (n. 110). *See also* R. Baldwin, M. Cave, and M. Lodge (n. 87) 108-9.
[112] Good governance can only be achieved if these three pillars are attended by the relevant policy maker: transparency, accountability, and participation. *See* De Hert, 'Globalisation, crime and governance: Transparency, accountability and participation as principles for global criminal law'. in C. Brants and S. Karstedt (eds), *Transitional justice and its public spheres: Engagement, legitimacy and contestation* (2017) 91.
[113] R. Baldwin, M. Cave, and M. Lodge (n. 87) 72-3.

of the criticism that certain regulator, such as the European Data Protection Supervisor (EDPS) and the EDPB[114], have already raised. In her excellent *Advanced Introduction to Privacy Law*, written based on a thorough understanding of the history of privacy, Megan Richardson contemplates the necessity to see new ideas on privacy protection developed. Sometimes these ideas are the result of a crisis, sometimes they are not and present themselves in a routine way and may grow over time.[115]

Using the work of Michel Callon, she points at processes of adjustment and readjustment as opposed to 'grand steps' that characterizes modern regulation.[116]

Wrapping up our third explanatory factor, we summarize that information and time limitations can partly account for the lack of guidance and creativity in the GDPR and other text regarding integrating data protection into novel data practices. That explanation might be benevolent to the regulator of the past but is not reason to sit still with a text of 2016. Like for the case of

[114] EDPB and EDPS, EDPB and EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), available at https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf (last visited 26 May 2021).

[115] M. Richardson, *Advanced Introduction to Privacy Law* (2020) 85. On the other hand, some legal changes seem to have happened in a fairly routine way, as for instance with the passing of the Human Rights Act in the United Kingdom, prompting *inter alia* a new tort of misuse of private information which has then been turned (along with data protection standards) into a legal tool to address contemporary issues. The long-gestated EU GDPR 2016 can be placed in the same category albeit on a much bigger scale. Indeed, quite often there is nothing that can be identified as a 'crisis', as such: rather it is just that with the benefit of experience of new technologies, practices and norms it becomes clear that new ideas are needed about how laws should be framed and applied in this environment. Or, as Lawrence Lessig put it in 1999, talking about the internet's open architecture as a threat to liberty, 'we are coming to understand a new powerful regulator in cyberspace, and we don't yet understand how best to control it' – and yet the threat to liberty was '[n]ot new in the sense that no theorist has conceived of it before. Others have. But new in the sense of newly urgent'.

[116] Ibid. 35. with ref. to Callon *et al*., 'The Management and Evaluation of Technological Programs and the Dynamics of Techno-Economic Networks: The Case of AFME.', 21(3) *Research policy* (1992) 215, at 215: 'We can use Lessig's analysis to imagine the effect of regulatory modalities on privacy subjects who may be constrained or enabled in their pursuit of privacy by the combination of technology, markets, social norms and law. This may occur in a range of ways, bearing in mind that, as Lessig says, the modalities do not only govern directly but also indirectly. For instance, privacy laws may be geared to influencing not just behaviour but social norms, technologies and/or market practices (and conversely the laws will also be subjected to influences from these other modalities). Moreover, the process of adjustment and readjustment will likely be an ongoing one. Or as Lessig puts it in *Codev2*, quoting Polk Wagner, "the interaction among these modalities is dynamic, <requiring consideration of not only . . . legal adjustments, but also predicting the responsive effects these changes will stimulate>, with the legal regulator seeking an <equilibrium> among the modalities. Thus, we can posit a dynamic feedback loop in which technological changes are followed by adjustments in markets, social norms and legal standards – examples of what French sociologist Michel Callon and his co-authors describe as <iterations>, movements to and for, negotiations and compromises of all sorts". The language suggests that changes will typically be more in the way of "iterations" than grand steps, that is, involving small incremental adjustments.'

data-driven practices, for some their effects are becoming apparent now and guidance is needed now.[117]

11 Closing Remarks: careful crafting and understanding regulatory modalities

In this longer study I looked at post-GDPR laws and the mess they create with regard to data protection law. My focus on the preservation in post-GDPR laws of the spirit and letter of the data protection law as incorporated in the GDPR has brought me to a critical diagnosis about mimesis as a recurrent practice without the noble art of legal integration. We are often *not* helped. We are sometimes even sent to the desert with small rhetorical tricks like 'nothing in this law is meant to derogate from the GDPR', leaving the citizen and norm addressee with many questions about the data protection practicalities, like what kind of consent is needed for data altruism in the DGA (section 5 and 7) and how many notification obligations do I have in case of a security breach (section 3).

What emerges from the examined post-GDPR laws in our case studies, the regulatory approach of EU law making agents shows patterns of GDPR mimesis and lack of substantive integration of those principles. I would reserve the term *mimicry* for those laws that mock with data protection, such as the Drone Regulations (section 4). The element of ridiculing suggested by the term *mimicry* is warranted because ridiculing is what these laws do: no taking the GDPR and its content seriously. *Mimesis*, the other term, is then reserved for many others post-GDPR laws with data protection relevance discussed in this contribution. Whether it is definitional, substantive, or symbolic, it should be dealt with suspicion. Only in cases where a real added value is envisaged, some mimesis is acceptable. In all other cases it is

[117] 'Consequently, when designing Big Data regulations, it seems advisable for governments to develop future-proof policies that follow and, where possible, anticipate this trend. If regulators only begin to regulate this phenomenon five or ten years from now, many of the projects will have already started. The negative impact may already have materialized, and it will be difficult to adjust and alter projects and developments that have already flourished. It should also be remembered that good, clear regulation can contribute to innovation and the use of Big Data. Since the current framework applying to new Big Data projects is not always clear, some government agencies and private companies are reluctant to use new technologies for fear of violating the law. New regulation could provide more clarity.' van der Sloot and van Schendel, 'Ten Questions for Future Regulation of Big Data', 7(2) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2016) 110, at 116. More nuanced on the regulatory void situation created by technological development, *see* R. Brownsword and M. Goodwin (n. 96) 371 and foll.

imitating a set of rules and principles with a high moral legitimacy, hoping that some of that bling would also work on other things. General disclaimers about the importance of the GDPR do not do the job and the argument that the DGA is also applicable to non-personal data (contrary to the GDPR) does not justify the lack of effort to integrate well.

Regulation should not be about bling, but about careful crafting and understanding regulatory modalities, without having necessarily the ambition for giant steps. Some of that care would be demonstrated by a concern for coherence and integration. In our discussion of the NIS Directive, we quoted Maria Grazia Porcedda who found notification duties in several EU laws all with the same objective to create more information or data security (section 3). Her final recommendation, to consider a unified law to address the issue information security and encourage the development of a mutual learning mechanism, is worth recalling in the conclusion of this study.[118] The EU has no criminal law code, no commercial code, no data protection code, … none of the kind. So, codification is hard to realize, and the idea of integration will have to be pursued differently. In the case at hand here, adding provisions to the GDPR, hardening certain rules that need hardening and explicit cross references to other post-GDPR laws, must be considered. A reverse exercise is to spell out in detail in all post-GDPR laws with what GDPR provisions they impact and how this data protection impact should be understood in an unambiguous way.

Approaches based on open-texture and EU wide agencification, as well as approaches based on mixing EU laws with other regulatory modalities combined with simple facts about the lack of legal creativity were discussed in the three last sections to contextualize post-GDPR law making, and to a certain extent, justify or topologically understand its attitude towards the boundaries of data protection law. Sociological insights about irritations (Teubner) and the slow speed legal insight (Michel Callon) indeed help to create a more realistic understanding of regulatory change. If there are no good ideas about regulating privacy aspects of drones about yet, then mimesis and promises about compliance with the GDPR might be all we have. My short, but benevolent discussion of AI reform (section 6) testifies for the capacity of the legal community to integrate well and to innovate legally, when all conditions are favorable.[119]

[118] Porcedda (n. 31) 1090-1098.
[119] In my first drafts I added other explanatory models based on path dependency, and the co-existence of critical junctures, but I decided not to include them and to invite critical readers to add their own explanations for regulatory developments with regard to data protection.

This said, there are reasons to understand the historical movement of the past years. With these three explanatory factors I drifted away from my previous research where, influenced by Bourdieu, I went after the question *who are the actors involved in regulatory change (who is the state) and why and how do they push for certain regulatory outcomes.* In this contribution that is part of a broader reflection on the boundaries of law. Let us come back to the actor perspective in our concluding paragraphs. What are the relevant facts?

One basic document, the GDPR, serves as a generic framework and a plurality of subsequent laws that apply this framework to (new) stakeholders, (new) political objectives (fairness of the market), and new developments in technology and societal practices (data altruism).

Each time, with every directorate launching a new proposal of a certain aspect of the data driven society, the GDPR is translated towards interpretations (templates, procedures, information notices etc.) by a different set of actors that shape personal data protection. Of course, all legal provisions, how clear voiced they may be, require interpretation by lawyers, judges, experts, or developers, shaped by and shaping social contexts. *Mimicri* and meaningless *mimesis* is guaranteed when these actors operating outside the data protection context are not motivated or challenged to apply a genuine data protection exercise.[120]

This calls for a specific, topological understanding of post-GDPR lawmaking at EU level. The sheer fact that the digital is now everywhere and that almost every EU-directorate has a portfolio affecting data protection demands for heighten concerns about integration and rent-seeking by interest groups within their familiar ecosystems far away from the state officials that traditionally discuss data protection (DG Justice; EDPS, EDBP, …). Interventions of data protection expert bodies like the EDPS or the EDBP in the legislative process, should therefore be singled out as of constitutional importance and should require more explicit attention for

[120] Breuer and Pierson, in their comparative analysis of smart city projects in two countries, reach a similar outcome: cities become smart without genuine data protection compliance whenever data protection experts of data protection savvy citizens are absent around the policy table. Data protection in policy and application contexts is always in a state of 'interpretative flexibility': semantic variations, or different interpretations, exist and groups compete to convince others. These actors interact with 'non-human actors' such as technologies and other artefacts (patents, contracts, other legislation, …) that together define and shape the respective ecosystems. See Breuer and Pierson, 'The right to the city and data protection for developing citizen-centric digital cities', 24/6 *Information, Communication & Society* (2021) 797 with reference social construction of technology-literature (Pinch and Bijker, 1984) and Actor Network Theory (Callon, 1990; Law, 2007; Lievrouw, 2014).

instance in the Recitals of EU laws. This and other ideas will make more meaningful coordination with the GDPR as a boundary setting instrument and subsequent laws possible.

In a past blog, my colleague Papakonstantinou wrote a particularly powerful concluding paragraph that I slightly reformulated and it sounded like this: *The GDPR is an immensely successful legal instrument that has a life and history of its own. EU personal data protection is currently busy tilting the planet towards stronger protection of the privacy of individuals under technological deluge. This seat is therefore taken. Any new EU regulatory initiatives will have to create a story of its own or better integrate in the consolidated GDPR mother story, and this, not by faking its appearance but by clarifying explicitly its implications for the new regulatory layer*.

12 Bibliography

A. Bradford, The Brussels effect: How the European Union rules the world (2020)

C. Joerges and E. Vos (eds), EU Committees: Social Regulation, Law and Politics (1999)

L. Fuller, *The Morality of Law* (2nd ed., 1964)

N. Luhmann, *Social Systems* (1995)