Technology and Regulation

The Regulation of Digital Technologies in the EU:

The law-making phenomena of "act-ification", "GDPR mimesis" and "EU law brutality"

Vagelis Papakonstantinou* & Paul De Hert**

EU technology regulation, act-ification of EU law, GDPR mimesis in EU law, EU law brutality

Evangelos.Papakonstantinou@vub.be

paul.de.hert@vub.be

EU regulatory initiatives on technology-related topics has spiked over the past few years. On the basis of its Priorities Programme 2019-2024, while creating "Europe fit for the Digital Age", the EU Commission has been busy releasing new texts aimed at regulating a number of technology topics, including, among others, data uses, online platforms, cybersecurity, or artificial intelligence. This paper identifies three basic phenomena common to all, or most, EU new technology-relevant regulatory initiatives, namely (a) "act-ification", (b) "GDPR mimesis", and (c) "regulatory brutality". These phenomena divulge new-found confidence on the part of the EU technology legislator, who has by now asserted for itself the right to form policy options and create new rules in the field for all of Europe. These three phenomena serve as indicators or early signs of a new European technology law-making paradigm that by now seems ready to emerge.

1. Introduction

EU regulatory initiatives on digital technologies has spiked over the past few years. On the basis of its Priorities Programme 2019-2024,[1] while creating "Europe fit for the Digital Age", the EU Commission has been busy releasing new texts aimed at regulating a number of topics, including, among others, data uses, online platforms, cybersecurity, or artificial intelligence.[2] This paper identifies three basic phenomena common to all, or most, EU new digital technologies-specific regulatory initiatives over the past few years, namely (a) "act-ification", (b) "GDPR mimesis", and (c) "regulatory brutality". These were first presented in three blog posts respectively, that were kindly hosted in the European Law Blog.[3] This paper further elaborates upon these three phenomena, taking advantage both of the academic exchanges that took place in the meantime and of the length of an academic article, that allows for more detailed analysis. Accordingly, in the following chapters each one of these phenomena will be elaborated separately, in consecutively numbered sections. Aim of each one of these sections is, first, to describe the phenomenon and, second, to place it within its proper theoretical framework. Finally, an assessment shall take place of whether the respective phenomenon, were its existence accepted, is positive or negative for the law-making purposes. While, in this manner, each one of the three basic sections of this paper is self-standing and independent from the others, a unifying approach will be attempted in the conclusions, where the point will be made of newfound self-assuredness from the part of the EU legislator, who by now seems confident enough to regulate new technologies in Europe practically in void, setting the pace for Member States instead of following them, as was the case in the not so distant past.

Apparently, a few clarifications need to be made beforehand, particularly on account of the vastness of each one of the topics to be discussed. The first, and most important one, pertains to what the authors mean when referring to "digital technologies". This is a far from resolved issue, even within a "Technology and Regulation" journal. While the authors adhere to this Journal's editor's opening remark about "*us*" being interested in "*technology with a capital T*",[4] the fact remains that outside the confines of "*our*" community[5] what "*technology*" includes each time may vary considerably. Aiming to avoid controversy, for the purposes of this paper the authors will focus only on

1 See the relevant European Commission's webpages at https://ec.europa.eu/info/strategy/priorities-2019-2024_en (accessed in Autumn 2021).

2 Therefore justifying mention of a "tsunami of digital legislation" (EDRi, *How it started, how it's going: Halfway through the current European Commission's legislative term,* January 2022, available at https://edri.org/our-work/how-it-started-how-its-going-halfway-through-the-current-european-commissions-legislative-term/).

3 Vagelis Papakonstantinou, 'The "Act-Ification" of EU Law: The (Long-Overdue) Move towards "Eponymous" EU Legislation' (*European Law Blog*, 26 January 2021) https://europeanlawblog.eu/2021/01/26/the-act-ification-of-eu-law-the-long-overdue-move-towards-eponymous-eu-legislation; Vagelis Papakonstantinou and Paul De Hert, 'Post GDPR EU Laws and Their GDPR Mimesis. DGA, DSA, DMA and the EU Regulation of AI' (*European Law Blog*, 4 January 2021) https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai; Vagelis Papakonstantinou and Paul De Hert, 'EU Lawmaking in the Artificial Intelligent Age: Act-Ification, GDPR Mimesis, and Regulatory Brutality' (*European Law Blog*, 7 August 2021) https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality

4 Ronald Leenes, 'Of Horses and Other Animals of Cyberspace' (2019) *Technology and Regulation* 1, 3 https://doi.org/10.26116/techreg.2019.001.

5 Again taken with a grain of salt, as identified by Leenes, Leenes (n 4) 5.

* Vagelis Papakonstantinou is a Professor of Law at the Faculty of Law and Criminology, Vrije Universiteit Brussel.

** Paul De Hert is a Professor of Law at the Faculty of Law and Criminology, Vrije Universiteit Brussel & an Associate Professor at the Tilburg Law School, Tilburg University.

Received 12 Jan 2022, Accepted 17 May 2022, Published: 21 May 2022.

information technologies, examining specifically newly released EU digital technologies' legislation. Consequently, it will be the Artificial Intelligence Act (AIA),[6] the Data Governance Act (DGA),[7] the Digital Services Act (DSA),[8] the Digital Markets Act (DMA),[9] the Cybersecurity Act[10] (or the NIS Directive,[11] as appropriate each time) and the Data Act[12] that will form the basis of their analysis while substantiating each of the three above phenomena. It is however well understood that even under this clarification this remains a highly selective, if not arbitrary, (and perhaps also self-serving, in order to serve this paper's arguments) process. The authors will of course stand corrected, and accept any criticism, for any omissions of digital technologies-related EU legislation or, on the contrary, EU legislation that is here considered as such while it can also be perceived as not.

A second clarification refers to the necessary limitations of an academic paper aiming to bring under the same roof three disparate phenomena, in spite of the fact that each one of them builds upon unrelated, and important, fields of law. Each one of the phenomena outlined in this paper would normally first require a thorough presentation of the respective legal background and state-of-the-art ("act-ification" would require an analysis on EU law nomenclature, "GDPR mimesis" on EU data protection law and "regulatory brutality" would first need an analysis on the relationship between EU and Member State law), before proceeding to make the argument that it is currently met in EU technology-relevant new regulatory initiatives. Obviously, such a detailed analysis would exceed by far the confines of an academic paper, especially if the main argument is to be highlighted and assessed. In this context, only brief mention of legal theory background for each phenomenon will be made here, with the aim of serving the main argument – even at the cost of sacrificing academic comprehensiveness along the way.

Finally, the last clarification pertains to the naming *per se* of these law-making phenomena. All three names ("act-ification", "GDPR mimesis" and "regulatory brutality") ought to be perceived only as simple naming conventions. They ought not be taken literally. The term *brutality* is used to refer to EU Commission's regulatory-instrumentalist mind-set, as eloquently identified by Roger Brownsword.[13] Nobody (certainly not the authors) could ever accuse EU law of actual "brutality", neither is the term "mimesis" used in its philosophical or artistic context. These three names originated from the needs of respective academic blog posts, but in the meantime, it was established that, for the moment at least, they serve their purpose well, in the sense that readers can almost immediately identify what is meant by them. It is to this end that their continued use is maintained also in this paper, however always paying attention at their limitations, and advising against taking them in their literal, scientifically accurate, meaning.

2. The "act-ification" of EU technology-relevant law: Eponymous vs. anonymous (numbered-only) EU legislative acts

2.1 The change of paradigm by the EU when regulating technology: "act-ification" at play

An emerging trend among EU lawmakers is to release eponymous new pieces of legislation for the regulation of digital technologies. These carry an easily identifiable name on their title, as opposed to the, still dominant otherwise, rule that all new EU legislation is anonymous, in the sense that it is only (consecutively) numbered. Specifically, the Commission over the past few years has released proposals for an Artificial Intelligence Act, a Digital Services Act, a Digital Markets Act, and a Data Act, while a European Cyber Resilience Act[14] is in the making. These important new regulatory initiatives followed the steps of the Data Governance Act and the Cybersecurity Act of 2019. The new trend shall be referred to in this analysis as "act-ification" of EU law, because of the recent surge on new EU "Acts".[15]

For the purposes of this analysis, eponymous EU laws are considered only those that formally and officially carry a name in their title. This is accomplished by means of parentheses that follow the "normal" name of the statute in question. In fact, the statute's name is provided in these parentheses, while the text preceding them describes their subject-matter.[16] If this is the case, the term "act" is a clear winner to any other alternative, such as "law" (see, for example, the European Climate Law[17]). The only competitor to such act-ification is the term "Regulation" itself, as, most notably, in the case of the General Data Protection Regulation (the "GDPR")[18] and the, still draft, ePrivacy Regulation.[19] However, as the above examples demonstrate, the EU Com-

6 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.

7 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final.

8 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/2020/825 final.

9 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.

10 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019.

11 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016 (NIS Directive).

12 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 23.02.3022.

13 Roger Brownsword, *Law, Technology and Society: Re-Imagining the Regulatory Environment* (Routledge, Taylor & Francis Group 2019) 195.

14 On 16 March 2022 the European Commission launched a public consultation "to gather the views and experiences of all relevant parties on the forthcoming European Cyber Resilience Act" (Press Release, 16 March 2022).

15 Taking into account developments until the time of publication of this paper, it could be claimed that the act-ification phenomenon became dominant in 2020 (broadly coinciding with the appointment of a new European Commission, in late 2019). After 2020, with the single exception of the NIS 2 Directive, all new regulatory instruments released by the Commission on digital technologies have been, effectively, act-ified.

16 In the same manner, simple and concise wording in the title of an EU act does not qualify. In this context, we were mistaken to classify the Regulation to serious cross-border threats to health (COM(2020) 727 final) and the Directive on the resilience of critical entities (COM/2020/829 final) in our blog post under the same phenomenon, because these two instruments merely carry a simplified name – they do not carry a formal title in parentheses, accompanying their description.

17 Proposal for a Regulation of the European Parliament and of the Council establishing the framework for achieving climate neutrality and amending Regulation (EU) 2018/1999 (European Climate Law) COM/2020/80 final.

18 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016.

19 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

mission has shown recently a strong preference towards the term "act" whenever naming a (draft) Regulation, although it would have been entirely possible to follow the example of the GDPR instead.

In all fairness, eponymous EU legal acts were not unheard of in the past. For example, the telecommunications and data protection community has long been acquainted with the ePrivacy Directive (or, more accurately, the "Directive on privacy and electronic communications").[20] Well-known is also the eCommerce Directive.[21] However, these by no means constituted either the rule or even a frequent occurrence. In their vast majority even famous EU laws only carried an informal name, that was formally used also by EU law-makers themselves (ie. the Commission) despite hesitating to include it in their formal title. For example, the NIS Directive that was released as late as in 2016, has been known as such by the Commission and practitioners alike,[22] despite of the fact that it does not carry this name on its title. On the contrary, the Commission could have rectified this situation in its amendment, still under discussion at the time of drafting this paper, that is conveniently referred to as "NIS 2" without nevertheless this name being introduced in its title.[23]

The examples of the NIS and NIS 2 Directives bring forward one more nuance of this phenomenon: In practice, it is Regulations that are "act-ified" by the EU legislator, not Directives. Perhaps this differentiation is nowhere more evident than in the case of the GDPR and the Data Protection Law Enforcement Directive.[24] While both instruments were released in 2016 at the same time, the Regulation did carry a formal name ('GDPR') while the Directive did not. Effectively, the Directive soon enough acquired a name as well, the "Data Protection Law Enforcement Directive",[25] but this is not a formal one. Taking into account also the NIS and NIS 2 examples above, it could be argued that this is a conscious choice by the EU legislator. Perhaps at an esoteric level the EU legislator views only Regulations as laws, on account of their direct effect, while Directives, that need to be applied at Member State level through local laws, do not merit such treatment. Whether this is a fruitful or not approach will be examined below, under 2.3.

Is this change of paradigm in EU law-making a digital technologies-exclusive phenomenon? Or is act-ification met in other fields of newly released EU law as well? While the authors do not claim knowledge of all fields of EU law, they would most likely reply in the positive: This indeed seems like a technology-only phenomenon, specifically aimed at regulating digital technology. Newly released laws in other fields of EU law are not so frequently named, if at all. For example, in EU banking and financial services law[26] legal instruments that were recently released, although rather suitable for making eponymous, decidedly avoided to do so.[27] Or, in the consumer protection law field recently released legal instruments that are referred to by name in the Commission's webpages[28] fail to carry such name formally in their respective titles. Same is the case in EU energy law, where, for example, the, informally named, Network Code on Electricity Emergency and Restoration,[29] is effectively a Regulation without a relevant title.[30]

The act-ification of newly released EU legislation on digital technologies becomes an all the more noteworthy phenomenon if one takes into account that Art. 288 TFEU does not speak of acts. Instead, it only mentions "regulations, directives, decisions, recommendations and opinions". Consequently, while the EU legislator follows the letter of Art. 288 (the persistent choice of Regulations to regulate new technologies to be discussed later, within the "EU law brutality" context under section 4), it consciously and persistently formally names them, using at all times the term act. In spite of the term "act" not appearing in the Treaties (other than as in "legislative acts") and the EU's Joint Practical Guide (JPG) disallowing the use of short titles in the manner preferred by the EU legislator (see 2.2), the fact remains that within new technologies, specifically digital regulation, act-ification is (almost invariably) at play. While the question why nomenclature in this case matters will be elaborated in section 2.3, a brief, but necessary, diversion will first be attempted into the naming mechanism of EU legislation, in order to demonstrate that the EU legislator apparently considers act-ification so important as to insist in it although this law-making technique is frowned upon by the relevant EU style guides, if not squarely forbidden.

2.2 Short titles in EU legislative acts

Titles are given to EU legislative acts according to the EU's Interinstitutional Style Guide (the "Guide").[31] The Guide is released by the Publications Office of the European Union, that carries, among others, the mandate to "standardize formats" and "harmonise the presentation of publications".[32] According to the Guide, the full title of an act comprises: (a) the type of act (regulation, directive, etc.), (b) the number, (c) the name of the institution which adopted it, (d) the

(Regulation on Privacy and Electronic Communications), COM/2017/010 final.

20 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002.

21 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000.

22 See, for example, the relevant webpages by the Commission at https://digital-strategy.ec.europa.eu/en/policies/nis-directive or the relevant webpages of ENISA at https://www.enisa.europa.eu/topics/nis-directive (both accessed in Autumn 2021).

23 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

24 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016.

25 See the Commission's relevant webpages at https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (accessed in Autumn 2021).

26 See the Commission's relevant webpages at https://ec.europa.eu/info/law/law-topic/eu-banking-and-financial-services-law_en (accessed in Autumn 2021).

27 See, for example, the Regulation (EU) 2019/1238 of the European Parliament and of the Council of 20 June 2019 on a pan-European Personal Pension Product (PEPP) PE/24/2019/REV/1, OJ L 198, 25.7.2019, that could have included a full title in the parenthesis but it failed to do so, limiting itself only to the PEPP initials.

28 See for example the Consumer protection cooperation Regulation (Regulation (EU) 2017/2394) or the Injunctions Directive (Directive (EU) 2020/1828) as referred to in the relevant Commission's webpages at https://ec.europa.eu/info/law/law-topic/consumer-protection-law_en (accessed in Autumn 2021).

29 See the relevant Commission's webpages at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum%3A4385118 (accessed in Autumn 2021).

30 Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration C/2017/7775, OJ L 312, 28.11.2017.

31 European Union, Interinstitutional Style Guide, Publications Office of the European Union, 2011.

32 See its relevant webpages at https://publications.europa.eu/code/en/en-000800.htm (accessed in Autumn 2021).

date of signature, and (e) an indication of its subject-matter.[33] In addition, "where the title of an act is amended by another act or is the subject of a corrigendum, the amended or corrected title should always be cited thereafter".[34] Implementation of the above has led to the multi-line titles of EU legislative acts with which we are acquainted today.

Additional guidance on the titles of EU legislative acts is provided in the EU's Joint Practical Guide (the "JPG").[35] After clarifying that "the 'title' comprises all the information in the heading of the act which serves to identify it",[36] the JPG continues to suggest that "the title of an act shall give as succinct and full an indication as possible of the subject matter which does not mislead the reader as to the content of the enacting terms. Where appropriate, the full title of the act may be followed by a short title".[37] Consequently, within EU nomenclature it is in the "short title" of legal acts where the phenomenon of act-ification is identified. Similarly, titles of EU legal acts are distinguished between the "full title" (points (a) to (e) above), the "title proper" (only point (e)), and their "short title", if any.[38]

The JPG is quite discouraging as regards short titles of EU legal acts: "A short title for an act is less useful in Union law — where acts are identified by a combination of letters and numbers (for example '(EU) 2015/35') — than in systems which do not have such a system of numbering. In certain cases, however, a short title has come to be used in practice (for example, Regulation (EC) No 1234/2007 = 'Single CMO Regulation'). Despite the fact that it may seem a simple solution, referring to acts by a short title creates risks for the accuracy and coherence of legal acts of the Union. This method should therefore only be used in specific cases where it significantly aids the reader's understanding".[39]

Apparently, there are two ways to introduce short titles in EU legislative acts, either in their full title or in their body. The JPG is even more condemning as regards short titles appearing on the full title of an act: "The creation of a short title when an act is adopted by adding it after the title of the act should be avoided, since it only renders the title more cumbersome, without actually resolving the question of whether or not the short title should be used, either in the act which created it or in subsequent acts. While the risks outlined in point 8.4 must always be borne in mind, it is possible to refer to an act by using a short title in order to make it easier to understand the act in which the reference is made. In this case, the short title chosen will have to appear in brackets in the body of the text of the act in which the reference is made, like any other abbreviation".[40]

While the merits of introducing short titles in digital technologies-related new EU legal acts will be discussed in the section that immediately follows, here it should be noted that the JPG does not provide any justification for its sweeping condemnation of short titles. Short titles are customarily used in the USA, although federal laws are numbered anyway.[41] In addition, it is not clear how addition of a short title "renders the title more cumbersome" while at the same time unnecessary information for the identification of a legal act is mandatorily included in its title, such as the institution(s) releasing it or any acts that are amended by it. Furthermore, the formalistic approach of the JPG is unmissable: Whether or not the short title should be used in the same act which created it or only thereafter is really a legalistic, trivial issue whose reply (that could go either way without any serious implications) is ultimately of minor importance when compared to the benefit the JPG itself admits, namely enhancing understanding. Finally, it should be noted that the JPG's request to include the short title in the body of an EU legal act and not in its full title has not been followed not only by any one of the abovementioned eponymous EU legal acts, but also(!) by its own example (the "Single CMO Regulation", that includes its short title in its full title).[42] At any event, in spite of the JPG's explicit (negative) approach, in the recent past the EU legislator has been consciously and persistently applying an act-ification approach while regulating digital technologies. An attempt to understand why such act-ification is as important to it to choose to deviate from the JPG is attempted in the following section.

2.3 Is "act-ification" when regulating technology in the EU helpful?

The obvious benefit of act-ification refers to awareness. Except to expert practitioners, numbers are hard to remember and use. It is one thing to refer to the "GDPR" and another thing to refer to "Regulation 2016/679". Short titles make it easier for the general public to refer to, and therefore use, legal acts in their daily lives.[43] This benefit ought not be underestimated. As noted by Mariachiara Tallacchini, public involvement and engagement has become the dominant paradigm in European institutional discourses.[44] However, the same author found out that similar exercises "have been mostly framed through highly specialized languages, with no concern for ordinary citizens and accessibility of the contents of the consultation".[45] If this is unavoidably the case in specialised, sector-specific legislation, when it comes to ambitious pieces of legislation that aim to regulate large swathes of everyday lives (such as, for example, the GDPR) it is important that their addressees can refer to them by name, in an accessible and memorable format. Recourse to a law is only possible when its intended recipients know it exists and are able to refer to it. Although sector-specific regulation addressed to a closed circle of stakeholders may employ whatever nomenclature it wishes, when large parts (or all) of society are the addressees of a certain piece of legislation ease of reference becomes of central importance.

Public awareness becomes particularly important whenever the EU is regulating digital technologies. Because technology invariably affects the operation of the Internal Market, regulating it falls within EU law competence. The EU has basically two regulatory vehicles to regulate digital technologies, either by means of Directives or Regulations. In

33 See Section 2.1 of the Interinstitutional Style Guide.
34 Ibid.
35 European Union, Joint Practical Guide of the European Parliament, the Council and the Commission for persons involved in the drafting of European Union legislation, Publications Office of the European Union, 2015.
36 See Guideline 7.1 of the Joint Practical Guide.
37 Ibid, Guideline 8.
38 See also idib, Guideline 8.6.
39 Idib, Guideline 8.4.
40 Ibid, Guideline 8.5.
41 See also Renata EB Strause and others, 'How Federal Statutes Are Named' 105 *Law Library Journal* 24. The discussion on the usefulness of short titles in legislative act is an old one, see, for example, A Symonds, 'The Mechanics of Law-Making' London 1835 (47).
42 Council Regulation (EC) No 1234/2007 of 22 October 2007 establishing a common organisation of agricultural markets and on specific provisions for certain agricultural products (Single CMO Regulation), OJ L 299, 16.11.2007.
43 This is a topic well developed in the USA, where naming statutes is the norm for reasons of awareness, accessibility and simplicity of reference (see, indicatively, Strause and others (n 47) 7ff.; Mary Whisner, 'What's in a Statute Name?' (2005) 97 *Law Library Journal* 182; Kent Olson, Aaron Kirschenfeld and Ingrid Mattson, *Principles of Legal Research* (3rd edition, West Academic Publishing 2020) 63].
44 Mariachiara Tallacchini, 'Medical Technologies and EU Law: The Evolution of Regulatory Approaches and Governance' in Marise Cremona (ed), *New technologies and EU law* (Oxford University Press 2017) 33.
45 Tallacchini (n 44) 33.

the not-so-distant past, Directives seemed to have been the obvious choice in this regard:[46] After all, personal data protection,[47] e-privacy,[48] cybersecurity,[49] databases,[50] and e-commerce[51] were all regulated by respective Directives until recently. Nevertheless, this is no longer the case: Since the release of the GDPR, Regulations have been the preferred regulatory instrument of the EU when regulating digital technologies. In practice, out of the aforementioned fields those who have witnessed their Directives being amended over the past few years (effectively, all with the exception of databases) have seen such amendment being performed through Regulations, not new Directives. Among them, the eCommerce Directive figures prominently, because its basic principles, that have had an important effect in regulating the internet,[52] are by now incorporated into an act (the DSA) and not a directive. It therefore appears that the EU, foreseeing harmonization problems, has been replacing Directives, that are apparently bound to perpetuate, if not exacerbate, the problem, with Regulations, whose direct applicability promises to resolve it once and for all. Under this perspective, if indeed harmonization is aimed at when regulating digital technologies in the EU, the use of Regulations appears to be a reasonable policy choice.

In this context, act-ification of all EU digital technologies-relevant law seems helpful. Regulations are directly applicable; Unlike Directives they do not need Member State laws to become applicable on the ground of EU Member States. In the past, when that was the case, public attention was turned to national, not EU, acts. For example, in the personal data protection field everybody in Europe knew of its existence however through reference to their national laws, not to the 1995 EU Data Protection Directive. On the contrary, once the GDPR was released each European became immediately acquainted with it by name.[53] By now public attention is captured by the GDPR, not each European's respective national law, although each Member State has invariably enacted one. Because it is the GDPR that directly applies and regulates relationships on the European streets, Europeans learned to refer to it directly instead of their national legislation. The same will presumably be the case with all other EU newly released draft Regulations, whenever they come into effect.

Once the act-ification process has been completed and all these instruments come into effect they will ultimately create a new European public space for the regulation of digital technologies. They will create a comprehensive European legal framework for the regulation of information technologies that will apply directly to all Europeans. This will inevitably move the public space, at least as regards digital technologies, from the local to the regional. It will no longer be national but EU law that will regulate directly the digital lives of Europeans, and Europeans will need to be aware of it. In order to do so, Europeans will need a memorable name to refer to. The term "act" denotes a law to any European, bypassing therefore national law nomenclature and local legal cultures. Similarly, avoidance of the term "Regulation" means that Europeans will not need to dive into the intricacies of EU law on whether a Directive or a Regulation is meant.[54] As such, therefore, EU's decision to release eponymous legislation for the regulation of digital technologies seems justified. Public awareness requirements mandated this policy option. Furthermore, preference to the term "act" rather than law seems equally justified, because the former is expressly referred to in the Treaties[55] and, as such, it has also found its way into the Guide and the JPG. In this context, act-ification of EU law means that the European public space that will soon be *de facto* created will become accessible not only to EU law experts but to its true recipients as well, the general public.

3. "GDPR mimesis" in (all?) EU technology-related regulatory initiatives

3.1 "GDPR mimesis": Has the GDPR's success dulled the EU legislator's imagination?

A second phenomenon that is viewable in the digital technologies-relevant regulatory texts examined above is "GDPR mimesis". The term "mimesis" is, of course, not used here in its literary, artistic meaning: in its true context it denotes "the act of representing or imitating reality in art, especially literature".[56] In this case, however, it is used purely to signify imitative representation.[57] The phenomenon of "GDPR mimesis" would therefore mean that new regulatory texts specifically aimed at regulating digital technologies imitate the GDPR.

To be able to identify GDPR mimesis we first need to distinguish the object of such imitative representation. In other words, what is there so unique in the GDPR that other regulatory texts strive to imitate?[58] While the EU personal *data protection acquis* and its embodiment in the GDPR will be examined in the immediately following subchapter, here it is noted that GDPR mimesis refers to the GDPR's regulatory approach. This is unique, and therefore identifiable, in the sense that, as noted by Yeung and Bygrave, "our examination of the GDPR's architecture [...] also demonstrates that the regime which the GDPR establishes is not readily characterized in terms of the kinds of binary distinctions often relied on in attempts to classify regulatory norms, modalities and

46 See, however, the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.
47 See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 (the "1995 EU Data Protection Directive").
48 See the ePrivacy Directive (n 20).
49 See the NIS Directive, (n 11).
50 See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996.
51 See the eCommerce Directive, (n 21).
52 See the Explanatory Memorandum of the DSA (n 8) 2 and 7.
53 See the Special Eurobarometer 487a (2019) on the GDPR, whose main finding was that "More than two thirds of Europeans have heard of GDPR".
54 Theoretically, a Directive could also carry the name "act", although, as seen under 2.1, this has not been the case so far.
55 See Art. 289 TFEU, referring expressly to "legislative acts".
56 Definition of mimesis from the Cambridge Advanced Learner's Dictionary & Thesaurus, Cambridge University Press.
57 See Oxford's Lexico at https://www.lexico.com/definition/mimesis, although it could be argued that law-making is a form of art (see, particularly, H Xanthaki 'Drafting Legislation: Art and Technology for Rules of Regulation' (Hart 2014) 10ff.
58 Thus making this a non-traditional exercise of comparative law, in the sense that instead of cross-border or cross-region comparative analysis of different legal instruments the provisions of same-jurisdiction legal instruments are examined with the purpose simply to reveal similarities; in addition, no policy recommendations are attempted either, thus replying in the negative Siem's basic question on "how far should the comparatist go"? (Mathias Siems, *Comparative Law* [2nd edition, (Cambridge University Press 2018] 27); From this point of view, the identification of the EU data protection acquis and its extrapolation onto other EU digital technologies' regulating instruments, basically formulating and then applying a high-level question ("are there similarities between the GDPR model and other EU models of regulating digital technologies?) would fall under a functionalist comparative law approach (Siems 32ff.). ; see also Koen Lemmens, 'Comparative Law as an Act of Modesty: A Pragmatic and Realistic Approach to Comparative Legal Scholarship' in Jacco Bomhoff and Maurice Adams (eds), *Practice and Theory in Comparative Law* (Cambridge University Press 2012) 319ff.

techniques".[59] If uniqueness *per se* is thus settled, in order to reply to the above question three basic forms of GDPR's "regulatory exceptionalism", and consequently types of mimesis, are hereunder identified: definitional, substantive, and institutional; it is these three that other technology-relevant EU regulatory instruments strive to imitate.

As regards definitional mimesis, the GDPR introduces a set of definitions that are not only unique to it but also create a specifically structured ecosystem whereby an identifiable decision-maker (the controller) affects passive recipients (data subjects) directly or through intermediaries (processors) while performing a specific, unique to the ecosystem act (processing of personal data).[60] As regards substantive mimesis, the GDPR sets its substantive law in terms of general principles and case-specific rules that are highly distinguishable, if not unique, to it. Finally, as regards institutional mimesis, the GDPR introduces an (again unique, in the sense of exclusive) new administrative system for its monitoring and enforcement. Consequently, it is against these criteria that each of the above instruments needs to be assessed in order to establish whether the phenomenon of GDPR mimesis occurs or not. However, it should be noted that is the totality of these three components that make up the GDPR mimesis phenomenon.[61] While it is true that each one of the above elements is not unique to the GDPR and that a number of other, unrelated EU laws also include in their bodies, for example, a set of case-specific definitions and/or establish a new public authority, it is their combined appearance that decides whether a new legal instrument imitates the GDPR or not. Positive resemblance needs to be visible, first, in their definitional approach, second, in their substantive provisions, and third, in the setting up of a new administrative monitoring mechanism. Only if all three conditions are met can GDPR mimesis be evidenced.

Keeping these in mind, in the case of the Data Governance Act the mirroring of the GDPR system is unmissable. As regards definitional GDPR mimesis, the DGA introduces a new, unique to it set of terminology in its Article 2, whereby "data holders" correspond to the GDPR's "controller", "data users" to "data subjects", and "data sharing" to "processing".[62] Then there is substantive mimesis: The DGA identifies a special set of principles to govern the provision of data sharing services[63] that resemble the principles relating to the processing of personal data in the GDPR;[64] The DGA, organizes a system for permitted data exports outside the EU[65] that reminds that one of the GDPR;[66] and, the DGA introduces a registry that each data processing organisation needs to keep internally,[67] that very much resembles the equivalent in the GDPR.[68] It should also be noted that the DGA relies heavily on a notification system,[69] that constituted the norm in the personal data protection field since the 1995 EU Data Protection Directive[70] and was only abolished in the text of the GDPR. Finally, as regards institutional GDPR mimesis the DGA establishes new state "competent authorities" to monitor all of the above[71] and also introduces a European Data Innovation Board[72] as a cooperation mechanism – the parallels to the GDPR monitoring and enforcement system at Member State and EU levels being obvious.

Similarly, the Data Act, that after all complements the DGA,[73] carries visible similarities with the GDPR. This is perhaps inevitable, given its scope: regulation of "access and use of data" unavoidably includes personal data as well.[74] Notwithstanding overlaps in scope, however, GDPR mimesis is evidenced through definitional mimesis ("data holders"[75] resembling the GDPR's "controllers" and "data recipients"[76] the GDPR's "processors"), substantive mimesis (the Data Act's rights of users corresponding to the data subjects' rights of the GDPR),[77] as well as, institutional mimesis (each Member State being obliged to designate a competent authority as responsible for the application and enforcement of the Data Act,[78] while DGA's European Data Innovation Board is to provide assistance wherever applicable).[79]

GDPR mimesis is also visible in the Commission's draft Artificial Intelligence Act.[80] Definitional mimesis may be evidenced through introduction of a new set of actors establishing an ecosystem that mimics that of the GDPR:[81] A "provider" is the decision-maker in this case, who either directly or through a series of intermediaries ("importer",

59 Karen Yeung and Lee A Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' 16 *Regulation & Governance* 1 https://doi.org/10.1111/rego.12401.

60 See Article 4 of the GDPR.

61 In this context, resemblances to other instruments of EU law that are visible but only partial are not examined under this text. For example, Veale and Borgesius have identified stark similarities between AIA's approach to manipulative systems (in Article 5) and the Unfair Commercial Practices Directive (Directive 2005/29/EC, Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' 4 *Computer Law Review International* 99; Similarly, enforcement procedures in the AIA carry obvious influences by the CPC Regulation (Regulation (EU) 2017/2394).

62 This was not an obvious choice by the EU legislator. The DGA could have furthered, or even replicated the Open Data Directive (Directive (EU) 2019/1024, yet another example of EU Commission informally naming of a Directive but otherwise hesitating to include such name in its title, see above subsection 2.1 on the NIS Directive(s))) with whom it is obviously, and expressly, related (see its Explanatory Memorandum). Or, it could have stayed closer to the FAIR data principles, from which it expressly "drew inspiration". On the contrary, the EU legislator opted for a new set of definitions, introducing new actors and ignoring those of the PSI/Open Data Directive regime, that broadly follow the allocation of roles in the GDPR.

63 See its Article 11.

64 See its Article 5.

65 See its Article 30

66 See its Chapter V.

67 See its Article 18.

68 See its Article 30.

69 See its Article 10.

70 See its Section IX. It should of course be noted that the 1995 Directive merely replicated a system that was already known and used in all European countries that enacted personal data protection legislation since the 1970s.

71 See its Articles 12, 13 and Chapter V.

72 In its Article 26.

73 See its Explanatory Memorandum, p. 4.

74 See, most notably, its Article 1(3).

75 See its Article 2(6).

76 See its Article 2(7).

77 See, for example, its Article 4 par. 1 on the right of users to indirectly access data or its Article 18 on compliance with requests for data or its Article 11 on technical protection measures on unauthorized use or disclosure of data.

78 See its Article 31.

79 See its Article 27 par. 3.

80 Something that was obvious also in the legislative proposals by the Parliament that preceded its release (see Vagelis Papakonstantinou and Paul De Hert, 'Refusing to Award Legal Personality to AI: Why the European Parliament Got It Wrong' (*European Law Blog*, 25 November 2020) https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong

81 In spite of the external similarities of the AIA with the New Legislative Framework (NLF), that are after all explicitly admitted also in its Explanatory Memorandum, the GDPR rights-based approach is unmissable: nowhere in the NLF, for example, are economic operators burdened with the principle of accountability, nor are NLF's enforcement authorities obliged to be "impartial and objective" nor does NLF's Union Product Compliance Network resemble in any way the AIA's European Artificial Intelligence Board.

"distributor", "authorized representative") affects passive recipients, the "users";[82] all of the above are engaged in using an "artificial intelligence system". From a substantive point of view, provisions in the draft AIA that are visibly affected by the GDPR (not including, of course, those provisions that directly refer to it, as is for example the case in Art. 10(5)) include, indicatively, the household exemption of Art. 3(4), the certification mechanisms (declarations of conformity and codes of conduct in Articles 48 and 69), the AI registration system,[83] the mandatory appointment of representatives in the EU for any AI non-EU actors,[84] or, perhaps most importantly, the principle of accountability.[85] Finally, institutional GDPR mimesis comes in the AIA in the form of supervisory authorities to be established at Member State level,[86] that are to be coordinated at EU level by a Board – in this case, the European AI Board.[87]

GDPR mimesis, however, is only partially visible when it comes to the Digital Services Act (DSA) and the Digital Markets Act (DMA), both instruments to be examined together, in view of them constituting "the Digital Services Act package".[88] At the same time as releasing its DGA draft the Commission also introduced its proposals for the Digital Services Act (DSA) and the Digital Markets Act (DMA). Both texts only partially resemble the GDPR model: in essence, although definitional and substantive mimesis are nowhere to be found, it could be claimed that the supervisory model introduced in the DSA, through the establishment of Digital Services Coordinators[89] to cooperate through a *quasi* one-stop-shop GDPR mechanism[90] and at EU level, through a European Board for Digital Services, fully qualifies for institutional GDPR mimesis. Why is there definitional and substantive GDPR mimesis missing for the DSA and the DMA? The reason could be attributed to path dependency: the DSA and the DMA, as was the case with the GDPR, have their own a long regulatory history. Particularly the DSA furthers and expands the eCommerce Directive. This e-Commerce Directive is an impressive text by its own merit that, same as the 1995 EU 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 sellers. Their definitions and substantive provisions could well be the result of path dependency within the same policy cycle, in the sense that they build on and further the aims and objectives of their predecessor, the e-Commerce Directive. While such path dependency is understandable, it might at the same time prejudice their approach; however, where an enforcement mechanism was missing from the e-Commerce Directive, their inspiration came directly from the GDPR, thus confirming their, admittedly partial, GDPR mimesis.

3.2 The *EU data protection acquis* and its embodiment in the GDPR

EU personal data protection law is a highly structured, and at times complex, legal system. From a hierarchical perspective at its top stands Article 16 TFEU, that is then consolidated for specific types of personal data processing through a number of regulatory instruments. The GDPR is only one among them; the Data Protection Law Enforcement Directive regulates personal data processing in the law enforcement field; Regulation 2018/1725[91] regulates the processing by EU organisations; a number of other instruments regulate either specific types of processing (e.g. relevant to Passenger Name Records – PNR) or specific agencies or bodies (e.g. Europol, Eurojust etc.). Countless other laws regulate personal data protection at Member State level. Nevertheless, it is the GDPR that has high-jacked global attention both in Europe and internationally. Perhaps because of its wide scope (it being accountable for most personal data processing operations) and its direct effect, the GDPR today constitutes the basic term of reference in order to denote EU personal data protection in general.

The GDPR does not hold its throne among all other EU data protection legal instruments unjustifiably. In essence, it embodies the EU basic regulatory approach to the processing of personal data. This approach was not created in 2016 but dates several decades back. In fact, it is built on premises as old as the first Hessian data protection act of 1970. Data protection laws were released during the 1970s and 1980s mostly with technology-regulation in mind. After an initial batch of similar laws was released during the 1970s (after Hesse followed Sweden, France and Germany), most other EU Member States followed during the 1980s. The formal EU approach to personal data processing came in 1995, through introduction of the 1995 EU Data Protection Directive. It is this Directive's approach that the GDPR expands and furthers, adapted to new technological and social challenges (most notably, taking into account that the 1995 Directive was drafted before the rise of the internet), encouraged of course by Article 16 TFEU that was introduced in 2008 through the Lisbon Treaty.

Consequently, the GDPR merely embodies (but does not, officially at least, formulate) the EU personal data protection system. It does so, however, in a most prominent manner, not only because of its fame and public acknowledgement, but also because of the detail of its provisions: compared to any other personal data protection instrument in effect in the EU today, the GDPR is the most comprehensive, most likely on account of its direct effect. Therefore, if it is accepted that anything like the "*EU data protection acquis*" has been formed by now, is needs to be looked for, first and foremost, in the text of the GDRP.

Whether an *EU personal data protection acquis* exists and, more importantly, what exactly it includes remains an open discussion. Its terminological existence ought not be doubted by now: The EDPS explicitly referred to it,[92] and the same has been the case in the not-so-distant past with the European Parliament.[93] The fact, however, that reference

82 A most notable difference with the GDPR being that the AIA does not afford rights to users (see Veale and Borgesius (n 61) 111).
83 See Article 51 and 60 of the Artificial Intelligence Act.
84 See Article 25 of the Artificial Intelligence Act.
85 See, for example, Article 23 or Article 26(5) of the Artificial Intelligence Act.
86 See Article 3(42) and 59 of the Artificial Intelligence Act.
87 See Article 56 of the Artificial Intelligence Act.
88 See European Commission, Shaping Europe's Digital Future, The Digital Services Act package, available at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
89 See Article 38 of the DSA.
90 See Article 45 of the DSA.
91 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018.
92 See, for example, the EDPS Opinion 2/2020, on the opening of negotiations for a new partnership with the UK, 24 February 2020.
93 See, for example, European Parliament, Resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)) available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0041+0+DOC+XM-

has been made to it does not also mean that its exact contents have also been defined. All of the above references are made in passing, without any further guidance as to what it is exactly that they refer to. Consequently, what an EU data protection acquis includes, and what it does not, is anybody's guess. Assistance can neither be found at global indexes, because of their generality: the United Nations'[94] or Greenleaf's[95] global metrics on countries that have enacted data protection legislation are fairly general in their classification criteria, understandably focusing more on the conditions under which any law qualifies as a data protection law than what exactly these laws include.

In view of the above, an *EU data protection acquis*, to be looked for in the text of the GDPR, would have to be derived through an analysis of its own provisions. Such an analysis divulges a well-known scheme by now: Building on a specialized, unique set of terms, a set of basic principles and case-specific rights are introduced, that are monitored by a specialized public agency. In some more detail, "data subjects" (meaning individuals) and "controllers" and "processors" (meaning those doing the processing) interact through "processing" of common or "sensitive" "personal information" (all terms closely, and uniquely, defined in the personal data protection context). This processing needs to be based on a set of special principles (e.g., fair and lawful processing, data minimization, purpose specification etc.). Special rights (e.g., information, access, rectification) need to be observed; specific regulatory tools (for example, impact assessments, data breach notifications, data exports' controls) complete the substantive law picture. All of the above are monitored by Data Protection Authorities, specialized state agencies that are established particularly for this purpose and carry out only this task. It is the totality of the above elements that formulates, to the authors' view at least and until a formal definition is released by the competent authorities, the *EU data protection acquis*.

Such an *acquis* is at the same time the unique identifier that sits at the basis of the GDPR mimesis phenomenon. As seen above, under subsection 3.1, GDPR mimesis may be identified through definitional, substantive and institutional striking resemblance of any new (digital technologies-related) EU initiative with the GDPR. Each one of these components corresponds to a distinct part of the EU data protection *acquis*. Its uniqueness and distinctiveness as met in the text of the GDPR consequently justifies identification of this phenomenon.

3.3 Strength in multiplication or forced replication that will lead to dead ends?

The GDPR mimesis phenomenon, were its existence accepted, raises inevitably the question whether the GDPR's success has dulled EU legislators' imagination, at least when it comes to the regulation of digital technologies. Is the GDPR's influence so dominant that each new EU regulatory initiative for technology and digital life is obliged to pay tribute to its *acquis* through replication? Is GDPR mimesis the only regulatory method when it comes to the regulation of digital technologies in EU law today?

An important point to be taken into account refers to the fact that the GDPR furthers a fundamental right, that of data protection. Consequently, as also noted by Yeung and Bygrave, "although the EU data protection regime is both technical and complex, drawing upon a range of techniques that combine both *ex ante* and *ex post* approaches, there is an underlying method to its apparent madness, underpinned by an overarching orientation that is primarily preventative".[96] Accordingly, both the DGA (and the Data Act) and the Artificial Intelligence Act adopt a predominantly preventative, protective approach for individuals. Their main concern is not to foster innovation[97] or enlarge the market but to protect individuals. Therefore, it could be claimed that GDPR mimesis is a phenomenon that is not met in any and all new digital technologies-relevant regulation in the EU, but only in those instruments aimed primarily at protecting individuals against digital technologies' imagined countereffects. Most likely, it is this protective, preventative *raison d'être* that throws them into the arms of the GDPR, as a model par excellence in this regard.[98]

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? Arguably, it does not. From a legal-technical point of view complexity is increased. If all of the above initiatives come through, definitional mimesis with the GDPR would mean in practice that the same company could be a "controller" or "processor" under the GDPR, a "data holder" under the DGA, and a "developer" under the AIA. Similarly, under a substantive mimesis lens, obligations could also cut across texts, at times on the same subject matter.[99] In this way, however, consistency – if it ever was an EU law objective at all, as most pertinently questioned by Brownsword[100] – would be substantially hampered. Finally, as regards institutional mimesis, is state agencies' inflation the EU response to digital technologies? Is it acceptable for the EU approach to new digital technologies to essentially comprise a highly structuralist, bureaucratic approach?

Even under a plain, human creativity perspective, mimesis is ultimately a bad thing. One is allowed, and indeed compelled, to stand on the shoulders of giants, but at some point he or she has to make his or her own contribution. Within a law making-context, Fuller has clarified that rules can be creative, but should be at least minimally clear and intelli-

L+Vo//EN accessed in Autumn 2021, as well as, European Parliament, Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0252+0+DOC+XML+Vo//EN (accessed in Autumn 2021).

94 See the UNCTAD's webpages on Data Protection and Privacy Legislation Worldwide, available at https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, (accessed in Autumn 2021).

95 See Greenleaf, Graham, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance (February 11, 2021). (2021) 169 *Privacy Laws & Business International Report*, 1, 3-5, UNSW Law Research Paper No. 21-60, Available at SSRN: https://ssrn.com/abstract=3836348 or http://dx.doi.org/10.2139/ssrn.3836348.

96 Yeung and Bygrave (n 66).focusing on the General Data Protection Regulation (GDPR

97 For example, the AIA, an expansive text of altogether eighty-five articles, includes only three articles with "measures in support of innovation" (53-55).

98 Whether this culminates into a European way to approach digital technologies in a preventative and defensive manner rather than in an exploitative and aggressive one (taking also into account the Commission's Declaration on European Digital Rights and Principles, COM(2022)28 final) merits further, comparative, research.

99 This is not an imagined risk; Already there is critical discussion on the relationship between the security requirements of EU data protection legislation and those of EU cybersecurity laws (see Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35 *Computer Law & Security Review*. Mark D. Cole, and Sandra Schmitz, The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape (December 31, 2019). University of Luxembourg Law Working Paper No. 2019-017, Available at SSRN: https://ssrn.com/abstract=3512093 or http://dx.doi.org/10.2139/ssrn.3512093).

100 Brownsword (n 13) 155.

gible, free of contradictions, relatively constant, and possible to obey.[101] Mimesis in any one of its forms (definitional, substantive or institutional), particularly among regulatory texts of different aims, scope and objectives, may lead to confusion through creation of unattainable public expectations. The GDPR has raised the bar considerably, for example educating individuals across Europe that a state agency can listen to their complaints and issue fines to infringers of their rights; An imitator, who also establishes such an agency but fails to equip it with similar powers, runs the risk of invoking GDPR mimesis without any of the GDPR benefits.

4. EU law brutality when it comes to regulating new digital technologies

4.1 Regulatory brutality in new digital technologies-relevant EU laws

The third phenomenon viewable in the technology-relevant regulatory texts examined above is "regulatory brutality". Here too, as was the case under GDPR mimesis, the term is not used literally: the authors under no circumstances claim that EU law is "brutal" or that EU law-making leads to "brutal" consequences for its recipients. Instead, the term is employed here within its "directness" and "difficulty" meaning:[102] "Regulatory brutality" denotes the almost complete disregard by the EU law-maker of Member States' own legal systems while regulating technology. In essence, new digital technologies-relevant regulatory initiatives by the EU legislator do not hesitate to introduce new terms, new procedures, new principles and new state mechanisms into Member States' legal system under a top-down approach that pays little attention to backwards compatibility's requirements.

The authors are of course aware that regulatory brutality in the above meaning is in principle impossible under EU law. Basic, fundamental safeguards underlie the whole EU edifice that are aimed at exactly that, the removal of any occasion where the EU disregards the legal systems of its Member States. This is achieved at the highest possible level both by means of fundamental principles and through institutional safeguards. Most notably, the fundamental principles of subsidiarity and proportionality[103] warrant that EU law pays attention to Member State law. From an institutional perspective, the participation of the Council of the EU in the EU law-making process warrants that Member State governments hold a decisive role while releasing new EU legislation. Similarly, the European Parliament is composed of directly-elected Members, thus warranting representation by Europeans in the same law-making process. Under these fundamental safeguards how could then one charge EU law, even when regulating new technologies, with regulatory brutality?

In fact, regulatory brutality neither contradicts the principles of subsidiarity and proportionality nor circumvents the Council or the Parliament. All the above safeguards are closely observed while releasing any new EU law, including these that regulate technology. Instead, regulatory brutality is noted not as regards the circumstances of their release but their substance, meaning their actual provisions. It is these provisions' "directness", "difficult(y)" and "indifference towards someone's feelings"[104] (which in this case are the legal systems in effect in each Member State), that are characteristic to it. In practice, regulatory brutality occurs when completely new legal systems, comprising new substantive law and new administrative mechanisms to apply it, are installed (or rather, superimposed) onto existing legal systems without much consideration for compatibility.

A few examples should illustrate this point better. In the field of cybersecurity EU law's first instrument was, arguably, the NIS Directive of 2016. The Directive introduced entirely new rules and definitions,[105] procedures,[106] and required from each Member State to establish internally a new state mechanism to apply its provisions.[107] At the time of its release most, if not all, Member States had no similar legislation in effect within their respective jurisdictions; at best, a few sectors (such as healthcare) had some obligations placed upon them by case-specific legislation,[108] but certainly nothing close to the scope of this new EU law. Consequently, an entirely new legal edifice had to be erected from scratch in each Member State, notwithstanding whether such Member State's legal system allowed for or was compatible to it. The same is the case in the DGA: It aims to introduce entirely new[109] rules and definitions,[110] principles,[111] and state mechanisms[112] that will be directly applicable onto Member States' legal systems notwithstanding of their readiness to receive them. Similarly, the AI Act too aims to impose upon Member States' legal systems new definitions,[113] new procedures[114] and principles,[115] as well as, a completely new state mechanism to apply all of the above.[116] In the past, similar has been the case, although on a much smaller scale, in the regulation of databases[117] or, even, ePrivacy legislation.

In all cases above regulatory brutality is showcased through introduction of new terms, new procedures, new principles, and new state mechanisms[118] into an already operating legal system under a top-down approach that pays little attention to compatibility requirements. Incompatibility can come in many forms. Notwithstanding budgetary constraints (new state mechanisms need money and human resources to run competently), legal constraints are subtler. For example, a specific new EU law term may be already defined in a Member State's law: e.g., it cannot reasonably be argued that such basic terms as "data" or "metadata" that are defined in the DGA have not been defined by any other Member State law so far. Or, it can be that a new EU law procedure directly contradicts existing procedures in certain Member States, for example while investigating an infringement or while

101 Lon L Fuller, *The Morality of Law* (Revised edition, Yale University Press 1969) 39.
102 See the definition of "brutal" in the Cambridge Academic Content Dictionary, Cambridge University Press.
103 See Article 5 of the Treaty on European Union.
104 See the definition of "brutal", above.
105 Namely, Digital Service Providers and Operators of Essential Services (see its Article 4).
106 Namely, mandatory development of a national strategy or incident notifications (see its Articles 7 and 14 respectively).
107 Namely, a new "national competent authority" and Computer Security Incident Response Teams (CSIRTs) (see its Article 8 and 9 respectively).
108 One should also keep in mind that EU law on critical infrastructures was issued as early as in 2008 (Council Directive 2008/114/EC), anticipating almost any Member State in this regard, therefore the same "brutality" phenomenon would be observed there too, although on a much smaller scale.
109 Nowhere in its Explanatory Memorandum does it mention any harmonization purposes among Member State laws.
110 See its Article 2.
111 See, most notably, the data altruism principle in its Chapter IV.
112 See its Article 12.
113 See its Article 3.
114 See, for example, classification of AI systems as high-risk.
115 See, for example, its Article 15.
116 See its Article 59.
117 Through the EU Database Directive, that introduced a *sui generis* right unheard of until then in Member States' national laws.
118 In the spirit of 'cooperative federalism', see Paul De Hert, 'EU Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the GDPR in the Spirit of Cooperative Federalism' in Stefano Montaldo, Francesco Costamagna and Alberto Miglio (eds), *EU Law Enforcement The Evolution of Sanctioning Powers* (Routlede 2021) 313.

establishing "main establishment" of legal entity. Or, in a case that has repeatedly given headaches to Member States and the EU alike, mandatory establishment of new "independent" state agencies, such as the Data Protection Authorities, to monitor a specific field does not sit well with the administrative structure already in place within any given Member State.

Contemporary legal systems, particularly well-developed ones such as those of EU Member States, are complex mechanisms with a long history and distinctive culture.[119] EU laws regulating technology ceaselessly challenge this edifice, by constantly introducing new terms and mechanisms under a top-down approach, without much consideration for each Member State's background.[120] Although the EU law supremacy principle will be discussed in the following subsection, here it is merely noted that in the past the EU intervened to Member State legal systems mostly through Directives, that afforded some space for manoeuvre and adaptation. Nevertheless, under the act-ification phenomenon discussed above, this is no longer the case. New EU laws regulating technology are mostly Regulations, that are directly applicable onto EU Member State jurisdictions – hence, the regulatory brutality.

Of course, one could argue that all the above new pieces of EU legislation regulating digital technologies, at least for the moment, are more high-level and technical than relevant to individuals. In other words, that they only install new structures and organisations in Member States without however being addressed to individuals, conferring them rights, and placing upon them obligations. Therefore, any EU regulatory brutality is nuanced, or even becomes insignificant, due to the limited impact on Europeans' everyday lives: all these new EU acts are aimed to operate in the background. It is a matter of lawyers and governments to best accommodate their requirements within their respective legal systems without citizens noticing anything.

While the above may be true for the moment, counter-examples do exist demonstrating that, even if at first new EU laws regulating digital technologies may lack brutality, this ceases to be the case later on during their lifecycle. Most notably, this is the case of EU personal data protection law.[121] At the moment of its introduction EU personal data protection law had been a notable exception to the regulatory brutality phenomenon, because instead of a top-down it was developed under a bottom-up approach. The 1995 EU Data Protection Directive is a notable case of technology regulation where the EU merely aligned and combined the approaches already developed among almost each one of its Member States.[122] Nevertheless, things changed drastically with the release of the GDPR. Practically all its novelties (data portability, the right to be forgotten,[123] data breach notifications etc.) were unheard of in Member States' national laws, that were until that time busy harmonizing themselves with the provisions of the 1995 Directive. The GDPR arguably struck Member States' national laws hard, not only on account of its many novelties but also because of its direct effect: Europeans may now refer to it directly, therefore legislators in Member States had no other option than to accommodate it within their national systems' particularities as best as possible.

What is critical when it comes to the regulation of digital technologies by the EU is that, in essence, the EU legislator (ie. the Commission) regulates in void. This is the result of two separate, unrelated between them, developments. First, all digital technology-related issues, being basically market related, broadly fall within EU law competence (with the, notable, exception of state security). Second, competing Member State law is either completely missing, due to the novelty of the sector that draws EU lawmakers' attention each time, or has such a short history that is not yet entwined into national legal orders creating insurmountable difficulties if replaced by new EU law provisions.[124] Consequently, the regulation of digital technology in Europe is not developed organically, first within each Member State and then harmonised at EU level, as would have been the norm, but is instead created from scratch under a top-down approach.[125] Taking this for granted, the EU legislator feels free to introduce new constructs and legal mechanisms to support its law-making options in what could be described as a brutal manner, in the sense that Member State particularities, whether legal, relating to public administration or of another kind, are in one way or another glossed over.

4.2 Supremacy invariably includes brutality, but that requires a conflict between two equal parties, and that is not the case in digital technologies' regulation in the EU

The principle of EU law supremacy (or, primacy) over Member State law is certainly a topic that largely exceeds the boundaries of this analysis. Here it is enough to be noted that this is a double-edged principle, in the sense that it simultaneously requires that the national legislator refrains from introducing laws that are inconsistent with EU law, and also that national courts set aside any national law that conflicts with EU law.[126] This is a principle that, notoriously, was developed not through explicit mention in the EU Treaties but through the case law of the CJEU.[127] Since the almost sixty years from its introduction it has

119 See also the "national identities" referred to in Article 4 par. 2 of the Treaty on European Union.

120 For example, in the case of personal data protection, Belgium had no experience in dealing with data protection infringements via administrative enforcement and administrative fines, but instead achieved protection through criminal sanctions, civil proceedings, and a Data Protection Authority without coercive powers; the GDPR, brutally, forced change upon this system (see, specifically, Paul De Hert, Complete Independence of national Data Protection Supervisory Authorities: About persons, czars and data governance in Belgian debates, (*European Law Blog*, 24 December 2021).

121 The same is the case with EU ePrivacy legislation, although within a much smaller scale.

122 At the time of its release only Italy and Greece did not have national personal data protection legislation already in effect.

123 Of course, Member States (specifically, their Data Protection Authorities) applied it already before the GDPR became applicable, but only as a result of the *Google Spain* case (CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, 13 May 2014) and not as a result of their respective national legislation.

124 See also the 'governance readiness' analysis by Andrews Leighton, 'Algorithms, Regulation, and Governance Readiness' in Karen Yeung and Martin Lodge (eds), *Algorithmic regulation* (Oxford University Press 2019), that includes 'regulatory capacity'.

125 Thus making it possible in the field of digital technologies for EU (supranational) law to fulfil the role usually reserved for national law, having addressed all three difficulties identified by Morgan and Yeung, namely absence of a single homogeneous "community" whose values are embodies in the law, absence of legitimate supranational institutions that enable policy trade-offs to be made transparently, authoritatively and in a manner which is responsive to the community, and, sector-specificity and policy fragmentation that tends to characterise the focus of supranational regulation. Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007) 304ff.

126 See Bruno De Witte, 'Direct Effect, Primacy, and the Nature of the Legal Order' in Paul Craig and Grainne De Burca (eds), *The Evolution of EU Law* (Second Edition, Oxford Univesity Press 2011) 340.

127 See Case 6/64, Flaminio Costa v E.N.E.L. [1964] ECR 585; See also, indicatively, Matej Avbelj, 'Supremacy or Primacy of EU Law-(Why) Does It Matter?: Supremacy or Primacy of EU Law' (2011) 17 *European Law Journal* 744, 744ff.; Monica Claes, 'The Primacy of EU Law in European and

fundamentally affected EU law, not only assisting its development but also bringing it on the ground at Member State level, in the sense that Europeans became directly affected by it.[128]

In the above sense, EU law supremacy invariably includes some regulatory brutality. Being prevalent and imposed on other legal norms or entire legal systems, it invariably requires that the latter are passed over, replaced, or made extinct. Notwithstanding the analysis whether this is ultimately the case with any legal system,[129] the fact remains that supremacy necessarily includes conflict and imposing the will of the winner unavoidably leads to regulatory brutality towards the norms found at the wrong side of the spectrum. What is important, however, for the purposes of this analysis is that supremacy or primacy requires two equal opponents. Or, even if not equal, then at least two conflicting parties. Or, EU law supremacy "*comes into play only when there is an actual conflict between two norms that are both capable of being applied to the facts of a case*".[130] Logically, therefore, primacy is irrelevant when only one player exists in the field.

This is exactly the case in EU's technology-relevant regulation: as seen above, most, if not all, new EU laws regulating technology do not have to deal with any Member State equivalents. They regulate their respective fields of activity from scratch, under a top-down approach. However, this is not what is expected under usual EU law circumstances: usually, Member States have well developed their own national laws, before witnessing them harmonized, or at any event brought together, through EU law. This bottom-up approach, that after all made rules to resolve conflict of laws necessary, is reversed in the regulation of digital technologies by the EU: in this case there is little or no national laws for EU law to be imposed on. In the absence of a local challenger, and therefore in lack of direct conflict, the principle of EU law supremacy does not apply.

Of course, such EU law making is in accordance with the fundamental principle of subsidiarity.[131] Pursuant to Article 5(3) TEU, "[u]nder the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level". As invariably discussed in the Explanatory Memorandums of all acts discussed in this paper[132] it is mostly such "reason of the scale or effects of the proposed action" that invites sole EU law-making on digital technologies. At the same time, however, one cannot but wonder whether the very nature of digital technologies themselves (or, essentially, of the internet) does not unavoidably make anything digital an exclusive area of competence for EU law or not.

At any event, what we are left with in practice when the EU regulates digital technologies is pure regulatory brutality. New regulatory systems, with their own definitions, principles and enforcement mechanisms, are superimposed onto Member State laws that have nothing comparable or even similar in effect. There can be no discussion of EU law primacy in this case because there is nothing conflicting with it in Member State law. On the contrary, there is brutality because entirely new legal systems developed centrally in Brussels have to be accommodated within each Member State's legal circumstances. They need to interact and interplay with them. However, because, by virtue of the act-ification phenomenon discussed above, EU law is directly applicable, there is not even the slightest space for flexibility for Member States. The local legal system needs to make space for the new EU laws as best as possible – the newcomer is not allowed to budge even an inch from its original position.

Some practical examples could illustrate the above point about pure regulatory brutality (or the combination of brutality and act-ification and mimesis) better. Under the GDPR mimesis phenomenon practically all new EU laws regulating technology establish new enforcement mechanisms to monitor their implementation at national level (see *above*). These new state agencies and their personnel are afforded with powers and privileges under EU law that may not be compatible with similar state agencies in each Member State. The act-ification phenomenon then forces each Member State to bend its own internal public administration rules to establish such new agencies as the EU law prescribes, rather than vice versa. Similarly, all of the above EU laws afford their respective enforcement mechanisms with one or another type of investigative powers; however, investigative powers as such may be exercised within any given Member State by specific state authorities only. By requiring an extension of alteration of these rules, EU technology-relevant law forces the national legislator to revisit the whole national system of state-run investigations. Or, by detailing the introduction of new certification mechanisms, EU technology-relevant regulation forces the national certification system already in place to adapt accordingly.

The same above examples are useful also in order to delineate the relationship between the brutality phenomenon identified here and full or maximum (or, for the same purposes, minimum) harmonisation in EU law. Within a maximum harmonization context, EU law allows practically no space for Member State law differentiations within a specific domain.[133] However, the level of differentiations (if any) is not at all of interest within the brutality phenomenon. It is not local regulatory autonomy that is at stake here. The brutality phenomenon takes any harmonization, regardless whether minimum or maximum, as a given. Instead, it focuses on the effect of newly released horizontal (broad-scope) EU law on existing Member State legal systems. The question then is, for example, not whether Member States are allowed to deviate, for example from the AIA provisions, and if yes, by how much.

National Law' in Anthony Arnull and Damian Chalmers (eds), *The Oxford Handbook of European Union Law* (Oxford University Press 2015).744ff.

128 See De Witte (n 126) 358ff.

129 See, indicatively, Justin Lindeboom, 'Why EU Law Claims Supremacy' (2018) 38 *Oxford Journal of Legal Studies* 337 with further bibliography.

130 De Witte (n 126) 342.

131 The principle of subsidiarity is a vast topic in EU law, constantly affected, and developed, by relevant case law as well; for a relatively recent update, summarizing also past views and critiques, see instead of all Federico Fabbrini, 'The Principle of Subsidiarity' in Robert Schütze and Takis Tridimas (eds), *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I* (Oxford University Press 2018).

132 See, for example, AIA's section 2.2 ("The nature of AI, which often relies on large and varied datasets and which may be embedded in any product or service circulating freely within the internal market, entails that the objectives of this proposal cannot be effectively achieved by Member States alone") or DMA's section 2 ("Digital players typically operate across several Member States, if not on an EU-wide basis, which, today, is particularly the case for services such as online advertising, online social networking services, online marketplaces, cloud computing services, online search services, video-sharing platform services, number-independent interpersonal communication services or operating systems").

133 In Weatherill's words 'a measure which asserts the EU as the exclusive site of rulemaking within the material scope [is described] as maximum harmonisation, while, by contrast, EU measures which permit scope for Member States to prefer stricter rules above the agreed EU norm will be called minimum measures' (Stephen Weatherill, 'The Fundamental Question of Minimum or Maximum Harmonisation' in Sacha Garben and Inge Govaere (eds), *The Internal Market 2.0* (Hart Publishing 2021); see also Stephen Weatherill, 'Consumer Policy' in Paul Craig and Gráinne de Búrca (eds), *The Evolution of EU Law* (3rd edn, Oxford University Press 2021) 898ff.

Instead, the question is how the AIA provisions themselves, being new and unprecedented within most (if not all) Member States' legal systems, interact with already existing and operating mechanisms. It is this interaction, that is inevitably brutal in the above sense, that is of interest here.

Admittedly the above examples do not pertain to the core of new EU legislation, but rather to its periphery. Nevertheless, they become important while applying it. Directors or employees within newly established agencies that cannot be properly placed under a public administration system will have trouble not only getting paid and insured, but also when interacting with (other?) civil servants. A mix-up in courts' and state agencies' roles means that significant delays will be caused to the very persons new EU laws wish to protect, meaning individuals. Certifications or other assisting mechanisms may take years to become effective, creating problems in the market anticipating them.

At the end of the day, regulatory brutality by EU law is a phenomenon viewable where no Member State law exists already. Nevertheless, the prevalence of technology has brought this phenomenon to the fore. While in the past fields where no Member State law existed were expected to be the minority, and thus EU law mostly held a reconciliatory, common denominator role, this is no longer the case, at least in technology-relevant fields. By now a complete reversal of roles has taken place. In part because of the pace of change and the significant resources needed to keep up, and in part because of the practical realization by Member States that EU law will unavoidably supplant or supplement their efforts soon enough,[134] technology-relevant law-making is, tacitly, left to the EU.[135] The importance of this finding is increased due to the increase of the importance of technology in our everyday lives. As a result, more and more new EU laws enter directly (through the act-ification" phenomenon) into the lives of Europeans. Because they are drawn from scratch under a top-down rather than a bottom-up approach, they inevitably develop a brutality effect by the time they land at Member States' jurisdictions.

4.3 Regulatory brutalism as the case where (Brownsword's) regulatory-instrumentalism hurts coherentism

In his seminal work *Law, Technology and Society*",[136] Brownsword constructs two ideal-typical mind-sets under which a legislator could engage with new technologies: under the mind-set of "regulatory-instrumentalism"[137] legal rules are seen as means to implement whatever policy goals have been adopted by the State; the adequacy and utility of the law is to be assessed by its effectiveness in delivering these goals. Under the "coherentism" mind-set, the adequacy of the law is to be assessed by reference to the doctrinal consistency and integrity of its rules.[138] The author then argues that a shift from a coherentism to a regulatory-instrumentalist mind-set is taking place, associated with the emergence of technologies.[139]

Brownsword, justifiably, develops his arguments within the context of a single jurisdiction. His examples are taken from EU law, remaining however at EU level. The relationship with Member State law is not examined. Assuming that Member State law, as an older system of law, has been developed under a coherentism mind-set, and that current EU technology-relevant law is being developed under a regulatory-instrumentalist mind-set,[140] what happens when the two (inevitably) collide? To our mind, it is then that the phenomenon of regulatory brutalism is noted. The EU wishing to reach specific results, through act-ification of its rule-making, imposes new rules and processes on Member State law, regardless whether these hurt the latter's coherence.

But, do the foregoing hurt the regulation of digital technologies? Notwithstanding the impossibility of agreeing what would actually hurt or benefit the regulation of technology, the fact remains that coherentism may be overrated while regulating technology: again in Brownsword's words, "*on the face of it, coherentism belongs to relatively static and stable communities, not to the turbulent times of the twenty-first century*".[141] If this is the case, then some regulatory brutality while implementing regulatory-instrumentalism by the EU may not be such a bad thing after all. New technologies raise new challenges, competitive regulation has become a global trend by now, and speed of reaction justifies some law-making violence in applying new norms in order to meet these challenges as best as possible. Regulatory brutality is therefore a necessary evil in the effort of Europeans to stay on the global top of regulating new technologies – if not imposing their own model to everybody else, under a "Brussels' effect" approach.[142]

There are, however, limits to such regulatory brutalism. Brownsword notes that "*whatever their [regulatory] interventions, they must always be compatible with the preservation of the commons* [the essential pre-conditions for human social existence] – *or, at any rate, with the relevant principles for the use of technological measures that have been agreed in a particular community*".[143] Indeed, regulatory brutalism is not allowed to go beyond this point, to break the basics of any particular Member State's legal system. Coherence within any legal system is important as such – regardless of whether one adheres to Dworkin's approach-,[144] the fact remains that, at least within EU law, coherence is proclaimed at the highest possible level: Article 11, para. 3 of the Treaty on European Union (TEU) states that "the European Commission shall carry out broad consultations with parties concerned in order to ensure that the Union's actions are coherent and transparent". Hence, coherence

134 Particularly taking into account that 'the EU better regulation system is one of the most advanced in the world' (Felice Simonelli and Nadina Iacob, 'Can We Better the European Union Better Regulation Agenda?' (2021) *European Journal of Risk Regulation* 11).

135 For example, in the case of AI regulation, Smuha notes 'Europe's intention to enjoy a first mover advantage in this regulatory field' (p.75), also taking for granted, within an AI regulation competitive context, that the EU speaks for all its Member States (Nathalie A Smuha, 'From a "Race to AI" to a "Race to AI Regulation": Regulatory Competition for Artificial Intelligence' (2021) 13 *Law, Innovation and Technology*).

136 Brownsword (n 13).

137 On 'instrumentalism' in the politics of policy instruments see also Stephen H Linder and B Guy Peters, 'Instruments of Government: Perceptions and Contexts' (1989) 9 *Journal of Public Policy*; as well as, Christopher C Hood and Helen Z Margetts, *The Tools of Government in the Digital Age: Second Edition* (2nd edition, Palgrave Macmillan 2007) 179ff.

138 Brownsword (n 13) 192.

139 Brownsword (n 13) 192ff.

140 See Brownsword (n 13) 196 on the Commission's 'perfectly clear' regulatory-instrumnetalist mind-set.

141 Brownsword (n 13) 198; For a discussion of the coherence test by the ECJ and the distinction between coherence and consistency see Hendrik M Wendland, 'When Good Is Not Good Enough: A Comparative Analysis of Underinclusiveness and the Principle of Coherence under Proportionality Review' (2018) 25 *Maastricht Journal of European and Comparative Law* 332; Stefano Bertea, 'Looking for Coherence within the European Community*' (2005) 11 *European Law Journal* 154.

142 See Anu Bradford, 'The Brussels Effect' in Anu Bradford, *The Brussels Effect* (Oxford University Press 2020).

143 Brownsword (n 107) 198.

144 Who 'famously argued that one of the characteristic aspirtions of legal (especially judicial) practice is that it should be principled in its approach, displaying a certain kind of integrity, and concomitantly that the body of legal doctrine (together with its underlying jurisprudence) should be coherent' (see, instead of all, Brownsword [n 13] 134 with further bibliography).

needs to be realized not as a blind standard for EU law making, but as a result from participative practice that includes the Member States. As such, coherence cannot be fundamentally challenged under a regulatory brutality acceptable level of intervention, no matter how justified in the case of technology regulation. The risk of damaging internal legal order in Member States and thus alienating its recipients, is much higher than the gains. Clear delineation between what is doable under Member State law to accommodate new EU technology regulation and what is destabilizing needs to take place – if by no other means, then perhaps through introduction of specific wording (ie. a new relevant principle) either in the very same EU laws that carry such brutality with them or, even, through amendment of the above Article 11 para. 3 TEU to read "the European Commission shall carry out broad consultations with parties concerned in order to ensure that the Union's actions are coherent and transparent, in particular in view of Article 4 para. 2".

5. Conclusion

The authors feel confident that the above phenomena remain visible and will not subside any time soon: the draft AI Act, that was released in Spring 2021, essentially vindicated all of them, carrying in its text all of their visible traits (namely, an "Act", that replicated many of the GDPR mechanisms and attempted to introduce entirely new rules and principles onto Member State national laws). Similar was the case with the Data Act, whose draft was released in February 2022. They therefore form consistent and persistent policy options of behalf of the Commission in its digital technologies' law-making programme.

If these phenomena are there to stay, what are we to make of them? In the authors' view, despite their varying nature, they all amount to new-found confidence on the part of the EU digital technologies legislator.[145] Act-ification denotes the willingness to develop legislation immediately accessible to and identifiable by all Europeans, instead of through the intermediary of national parliaments as was the case until today (and remains, in non-technology domains). GDPR mimesis divulges confidence on a successful EU model of regulation to be replicated in other, neighboring fields as well. EU law brutality reveals a willingness and readiness to create new rules and impose them onto national legal systems no matter the cost. None of these traits were present a few years back and none of these traits were altogether visible in other domains where EU law is also competent. It is technology regulation that has taken the lead, shifting towards a new paradigm in EU law-making.

In order for the above phenomena to fully develop their potential a number of modifications would be advisable. In the case of act-ification, a re-write of the JPG to accommodate and institutionalise this new trend would benefit not only the EU legislator but also Europeans, being the ultimate recipients of such rule-making. In the case of GDPR mimesis, continued studies, along the lines discussed by Yeung and Bygrave above,[146] are needed in order to properly assess whether the GDPR system is indeed worthy of replication when regulating technology and whether its unavoidably protective perspective does not affect negatively European approaches on new digital technologies. Finally, in the case of EU law brutality, the direct confrontation on many fronts of new EU technology law with Member State legal traditions makes formulation of an explicit new EU law principle, giving precedence to the former but respecting the latter, more relevant than ever. At the end of the day, co-existence of legal rules and spheres within the context of a "cooperative federalism"[147] could help reduce friction.

Ultimately, however, the above phenomena bring forcefully to the fore the question already identified by Brownsword a few years back, that remains unanswered until today: What kind of Information Society Europe wants.[148] Act-ification and EU law brutality mean that the EU legislator has asserted for itself the right to form policy options and create new rules in the field for all of Europe. However, the direction these will take remains an open issue. GDPR mimesis perhaps means that a protective rather than a full-blown capitalist approach is preferrable to Europeans – but, as seen, exceptions do exist, making this a far from uncontested policy choice. What cannot be contested, however, is EU's increased pace of releasing technology-relevant regulation, even if a unified strategic approach is still missing. The three phenomena identified in this paper serve as indicators or early signs of a new European technology law-making approach that by now seems more ready than ever to emerge.

145 Such newfound confidence to make Anu Bradford 'even see a magnified "Brussels effect" on global digital policy compared to the many other areas in which the EU already exerts a significant "normative power Europe"' (noted by Andrea Renda, 'Single Market 2.0: The European Union as a Platform' in Sacha Garben and Inge Govaere (eds), *The Internal Market 2.0* (Hart Publishing 2021).

146 Yeung and Bygrave (n 59).

147 See De Hert (n 121).

148 See Brownsword (n 13) 332ff.