Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

SCHOOL OF LAW

LEGAL STUDIES RESEARCH PAPER SERIES

PAPER NO. 17/2023

December 2023

[Conclusions of 'Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis']

[Maria Grazia Porcedda, Trinity College Dublin]

Further information about the Trinity College Dublin School of Law Legal Studies Research Paper Series can be found at
www.tcd.ie/law/researchpapers/

Conclusions of 'Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis'

Maria Grazia Porcedda*

[This is a draft of the conclusions of the monograph *Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis* (Hart Publishing 2023).]

I. Summary of findings

How are cybersecurity, privacy and data protection (the triad) reconciled in EU law? This is the question I sought to answer with this book, a question that becomes more pressing by the day as our lives, society and democracy become intertwined with networked information technologies as critical infrastructure. Studying the relationship of the triad is no easy endeavour because in cyberspace, information and data can cause the triad to both clash and converge. To investigate the triad's relationship, I conceptualised the ambivalence caused by clash and convergence along an axis, shown in Figure 1, ranging from no to complete reconciliation and particularised by five relational modes.

Reconciliation				
None		**Weak**	**Strong**	**Complete**
<----------				---------->
Clash		***Indifference (non-interference)***	***Complementarity***	
Zero-sum	Balancing		Convergence	Overlap

Figure 1 Modes of reconciliation of the triad

* Assistant Professor in Information Technology Law, Trinity College Dublin, the University of Dublin, Ireland [ORCID: 0000-0002-9271-3512].

To the far right is strong reconciliation underscored by complementarity. 'Overlap' expresses the idea that cybersecurity, privacy and data protection are different facets of the same thing, thereby enjoying complete reconciliation. 'Convergence' points to the triad's shared goals and therefore underscores synergy and complementarity. To the far left is weak reconciliation underscored by clashes. 'Zero-sum' expresses the irreconcilability of the triad, while 'balancing' refers to the method of adjudication incorporated in the proportionality test characterising a mode of co-existence in which something has to give. An in-between state classed as 'indifference', for want of a better expression, points to reciprocal non-interference.

Some modes of reconciliation are not viable in all jurisdictions. The research question builds on the assumption that zero-sum outcomes are not compatible with EU law and the reasons why this is the case bring to surface elements for an analytical framework to investigate what other modes of reconcilability apply. To ascertain the modes of reconciliation, it is necessary to examine cybersecurity, privacy and data protection as: (i) techno-legal objects situated within the EU constitutional architecture or *ordre public* underpinned by the rule of law (RoL) and the EU multilevel system of protection of human rights; (ii) the values the triad expresses; and (iii) their concrete policy substantiation. The latter includes looking at the applicable laws (high level of abstraction) as well as their implementation (low level of abstraction) with an eye to technology. To treat cybersecurity, privacy and data protection as situated techno-legal objects of enquiry one must look at each separately and as they interact in the Digital Single Market (DSM), the Area of Freedom, Security and Justice (AFSJ) and External Action (EA) through policy, law and technology, bearing in mind the idiosyncrasies of such areas of EU decision-making.

In part one of the book (chapters one to four) cybersecurity, privacy and data protection were examined as self-standing regulatory objects. The analysis of cybersecurity in chapter two pointed to a framework still in the making and characterised by plasticity. The term 'cybersecurity' encompasses Network and Information Security (NIS), the fight

against cybercrime, the collection of e-evidence, cyberdefence and cyberdiplomacy, cyber-exports and it can even incorporate elements of privacy and data protection. All dimensions of the Cybersecurity Policy come together, to the extent that treating them separately is an artificial exercise. Such plasticity is reflected in successive EU Cybersecurity Policies, with the 2020 Policy placing special emphasis on the synthesis of dimensions. However, the open-endedness of the concept of 'cybersecurity' betrays the cacophony of interests generated by communities animating its different facets. Moreover, as the development of the cybersecurity policy intersects with the peculiar evolution of the DSM, AFSJ and the EA, the result is a patchwork of instruments displaying both connections and clashes within and across areas of policymaking.

Privacy and data protection are treated as interlinked but independent rights enshrined in Articles 7 and 8 CFR,[1] each endowed with essential components and one or more core areas as identified by the CJEU. In both cases, essential components are enriched with findings from secondary law. Also in both cases, vagueness as to the essence favours an 'evolutive' interpretation of the two rights but weakens the possibility to understand whether measures stemming from legislation, including technologies, are proportionate and impose clear and strict permissible limitations.

Chapter three reviewed the connection between Articles 7 CFR and 8 ECHR[2] to identify privacy's essential components. The analysis points to a smaller scope of Article 7 CFR than Article 8 ECHR. The right's essential components are drawn from the four limbs of the right – private life, family life, home and communications. Private life is further conceptualised into physical and psychological integrity, personal social and sexual identity, and finally personal development, autonomy and participation ('outer circle'). The pronouncements of the CJEU point to three elements of the essence: [the revelation of] very specific information concerning the private life of a person, not limited to certain

[1] Charter [2012] OJ L326/391 (CFR).
[2] Council of Europe, ETS no.° 005, 4 November 1950 (ECHR).

aspects of that private life; for a father, the possibility to apply for the right to custody; and the content of communications.

Chapter four looked at data protection as a self-standing fundamental right, the independence of which is worth defending even in the face of ambivalent case law of the CJEU. The right has four essential components roughly corresponding to the three paragraphs of the right: protection, legitimate processing (fairness, lawfulness and purpose limitation), data subject rights and independent control. Essential components tend to have a manifest content but are also capable of subsuming other meanings, as found in secondary law or court decisions. For instance, protection reflects both the architecture of personal data protection and, in a more restrictive sense, the principles and related technical and organisational measures (TOMs) to safeguard individuals against harms that may derive from processing. The provision in the legal basis of measures protecting the integrity and confidentiality of data are an element of the essence, as are measures effecting purpose limitation. The overlap between independent control and data subject rights can give rise to a right to human oversight or intervention, at a minimum to explain the functioning of the processing so as to give meaning to the right to access to one's data.

In part two of the book (chapters five to eight), the common reference to confidentiality and, to a lesser degree, integrity across the triad emerging from the analysis offers the opportunity to investigate a possible overlap. This was done in chapter five through a techno-legal prism comparing both the technical understanding of the triad drawn from threat modelling – including security properties, protection goals and design strategies – and legal understanding of the rights as endowed with essential components and essence. If overlap appears to be a possible mode of reconciliation in theory, it is difficult to prove that in practice due to the lack of a common vocabulary between technologists and legislators, the misalignment between risk management and proportionality tests and some recurring features of (networked) information technology law.

Network and information technology as a regulatory target was dissected with a focus on two regulatory strategies, technology neutrality (TN) and 'by design'. Such regulatory strategies serve delegatory co-decision frameworks, which are studied by different bodies of literature. In a nutshell, secondary legislation creates the framework outlining the goals to be achieved and harms to be avoided[3] through the implementation of TOMs selected in accordance with a dynamic 'state of the art' (SoA) set by Standards Setting Organisations (SSOs) and Standards Developing Organisations (SDOs). Following the TN principle, the law only sketches the parameters of TOMs, which should abide by set principles 'by design'.

However, requirements couched in technology neutral terms frustrate efforts to align the design of TOMs to such requirements; furthermore, TOMs are destined for technology users rather than developers. The European data protection by design Standard adopted in 2022 notably 'provides voluntary tools to manufacturers and service providers to allow them to demonstrate to controllers'[4] compliance with 'by design' principles. The standard does not aim to provide a presumption of conformity and is not for publication in the Official Journal. The data processing, software-driven component of information technologies has further eluded stringent legislation on account of its misalignment with existing categorisations of product, process, service or system.[5] What is more, SSOs and SDOs are populated by actors that also happen to be among the major addressees of secondary legislation as technology users while also being information technology developers. Consequently, the law delegates to its most powerful addressees both the choice of what TOMs correspond to the SoA and what values are embedded in TOMs and how.

[3] Developing the work of J Black 'The Emergence of Risk-Based Regulation' [2005] *Public Law* 512, see R Gellert, *The risk-based approach to data protection* (Oxford,Oxford University Press, 2020).
[4] European Commission, 'Commission implementing decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy. Mandate M/530', 5.
[5] Regulation (EU) 1025/2012 [2012] OJ L316/12.

Such dynamics effect an ironic 'effacement of technology' from technology law and a 'technology indeterminacy loop'. Higher courts such as the CJEU and the ECtHR only review the legality of measures that are enshrined in law, so that the law's technological implementation disappears beneath the courts' radar and fails to contribute to the binding interpretations of the law. Thus, courts are not put in the position to supplement legislation with workable criteria that bridge law and technology; to the extent they ignore such dynamics, balancing formulas devised for the digital age are incapable of redressing the indeterminacy loop.[6] This, among other reasons, hampers the development of a common vocabulary between technologists and legislators and thus the demonstration of overlap. Such a finding also raises questions as to the possibility to define a default mode of reconciliation of the triad at high (applicable law) and low (technology implementation) levels of abstraction.

The investigation as to the mode of reconciliation of the triad continues with a study in chapters six to eight of the interaction of the triad in the DSM, AFSJ and EA, including the Common Foreign and Security Policy (CFSP) through policy, law and technology. In all areas, policy documents offer an overview of the context in which the relationship of privacy and data protection with NIS, the fight against cybercrime and collection of e-evidence as well as cybersecurity in the international arena play out.

The analysis shows substantive and procedural functional interconnection between NIS and cybercrime instruments in the AFSJ and EA. In particular, the pursuit of NIS and the response to cyber-dependent or 'narrow' cybercrime are functionally interconnected as to their substance, while the investigation and prosecution of all cybercrimes, collection of e-evidence and CFSP restrictive measures are functionally interconnected as to procedure. Such interconnections seem to relate to strong or weak reconcilability at a high level of abstraction. Instruments dealing with substantive matters point to strong reconcilability

[6] M Susi, 'The Internet Balancing Formula' (2019) 25 *European Law Journal* 198–212; R Alexy, 'Mart Susi's Internet Balancing Formula' ibid| 213–220.

between the triad: frameworks converge on common goals and underpin the mutually beneficial nature of cybersecurity, privacy and data protection, although with caveats.[7] Conversely, rules enabling the collection of e-evidence point to weak reconcilability: frameworks pursue different goals, are fragmented and underpin the need to balance cybersecurity, privacy and data protection. And yet, such interconnections are not enough to determine the relationship of the triad.

With respect to NIS, the analysis of policy and especially law showed strong reconciliation of the triad in the applicable law but not when considering technology as an element of implementation. Principles of EU policymaking informing the technological implementation of the applicable law and effecting the effacement of technology prevent strong reconciliation, as shown by the analysis of deep packet inspection. In the AFSJ, the analysis of policy and law underscored different degrees of reconcilability between measures addressing cybercrime, privacy and data protection depending on the goals of specific instruments. The spillover effect of the 'effacement of technology', if subdued on account of the reach of EU law in the AFSJ, prevents strong reconciliation, as shown by the analysis of deep packet inspection. Such variety, ranging from strong reconciliation to classic balancing, reflects the intrinsic complexity of cybersecurity as a policy area. Unresolved policy tensions reverberate through secondary law, to the detriment of coherence and legal certainty.

For both NIS and the AFSJ, the concept of the 'essence' appears unable to act as a fail-safe mechanism. The lack of technological specificity in the pronouncement of the CJEU creates a porous border between content and metadata, begs the question of whether there is a quantum of information capable of providing very specific information about one's private life, does not refer to a minimum threshold for confidentiality and integrity requirements and challenges the feasibility of stringent purpose limitation requirements in practice. With such loose parameters, the technological implementation of measures

[7] NIS instruments prioritise continuity of service, while fundamental rights prioritise fundamental rights. See ch 6, section III.D.

escapes a rigorous assessment; measures capable of infringing privacy and data protection and of constituting an 'attack' against network and information systems are not nipped in the bud. Rather, they are allowed to flourish until they become mainstream and too entrenched to be removed,[8] even if their use is not only capable of interfering with rights, but also of affecting their essence.

The analysis in chapters six and seven also draws a trajectory: reconciling cybersecurity, privacy and data protection becomes increasingly challenging as we move from older to newer EU policy areas, where integration is weaker and national variations are more entrenched.[9] Such dynamics affect external policymaking, with tensions that have been left unresolved internally likely to be replicated externally. The study of the EA proved more complex than NIS and cybercrime on account of the breadth of the area, the range of instruments and the need to consider the external dimension of NIS and cybercrime instruments. An analysis of restrictive measures points to the validity of functional interconnection in the EA; the examination of frameworks such as export controls on dual-use technology could further confirm the finding.

The analysis of the EA casts the 'effacement of technology' from technology law under new light. The ability to translate norms into practice depends on both standard setting and technology leadership. Standards, which are adopted by public or private international bodies, have gone from harbingers of international free trade to tools of political influence. Technology leadership over 'high-tech' products,[10] which has always been a field of geopolitical competition, is now fully concerned with data flows as crucial to innovation. The physical, logical and social components of cyberspace[11] have all become relevant to the

[8] Eg, following the Collingridge dilemma and similar arguments (see ch 5, sections III–IV).
[9] M Cremona, 'The Union as a Global Actor: Roles, Models and Identity' (2004) 41 *Common Market Law Review* 553–573.
[10] H Nau, *National Politics and International Technology* (Johns Hopkins University Press, 1974); J Lembke, *Competition for Technological Leadership* (Cheltenham, Edward Elgar, 2002).
[11] MN Schmitt (ed), *The Tallin Manual 2.0 on the International Law Applicable to International Jurisdictions* (Caambridge, Cambridge University Press, 2017), 12.

maintenance and consolidation of state power, as exemplified by the mainstreaming of terms such as 'technology' and 'cyber' sovereignty.

The EU displays great influence as a norm-setter, especially for what concerns privacy and data protection, although a number of key regulatory principles including the TN and by design principles are normative imports. By contrast, the EU is a weak contributor to standards and a technology follower. Such a reality is painfully depicted in the 2020 Cybersecurity Strategy, with interventions that appear better suited to treat symptoms rather than cure causes. The causes of the hiatus between norm-setting and standards/technology-taking are rooted in dependence on technological systems provided by the market that are far removed from the norms enshrined in primary and secondary legislation and procedures unable to provide corrective measures because they assign the solutions to…the market. What is more, Brenner notes how states turn to 'corporations as the twenty-first century "nobles" the resources of which nation-states employ to control cyber-threats'.[12]

In sum, the default mode of co-existence of the triad in EU law is weak reconciliation. Some technological applications are even capable of creating zero-sum games, which go undetected due to the effacement of technology from the law. Although overlap is difficult to achieve in light of the conflicting aims of cybersecurity, strong(er) reconciliation between the triad could still be possible if legislation consciously steered the technological choice and development of network and information technologies and cyberspace.[13] Such intervention concerns the entire lifecycle of a technical measure, from its design to its implementation and the applicable law under which the measure operates. The techno-legal analysis discussed in chapter five, which connects the essential components of rights with technological principles, could provide a first approach to operationalise values to embed in technology, to supplement fundamental rights impact assessments and to inform tests for

[12] S Brenner, *Cyberthreats and the Decline of the Nation-state* (London, Routledge, 2014) 162.
[13] For those familiar with the etymological origins of cyberspace from cybernetics, drawn from the Greek kubernētēs 'steersman', the pun is intended.

permissible limitations that favour the most protective technologies.[14] But any method ultimately requires making technology 'reappear', by revisiting our legal analytical categories and our way of 'making laws for cyberspace'.[15]

Our way of making laws for cyberspace is possibly broken. The specifics of technology and possible usage are not subsumed under TN concepts such as state of the art, technical measure, organisational measure, content and monitoring; European judges (CJEU and ECtHR) are not put in the position to take responsibility to fill the vacuum and thus the test for permissible limitations, which is tech-agnostic, as are proposals for balancing in the digital age, provides little guidance; and rights are open-ended. What is more, these trends are mutually reinforcing. At the lower level of abstraction, courts do not perform an analysis of the technology involved because the applicable law is silent on that point; at a higher level of abstraction, courts do not provide a clear interpretation of rights, partly because of the 'living instrument' doctrine. While this enables adapting rights to changing times, it creates such a degree of uncertainty that can ultimately seriously undermine the enjoyment and substance of rights, without necessarily increasing the level of cybersecurity. Indeed, against this background, the market has free rein to identify sub-standard solutions that suit the agendas of different communities, whose interests may prevail over the reconciliation of the triad. As the cybersecurity market is notoriously characterised by a high degree of failure, it is unlikely that a solution will be found there, certainly not without remedial action.

What, then? Geopolitical and economic factors and extant technology law approaches affect political willingness and the options available to adopt interim solutions – be they technology-specific law, technological committees or specialised courts – and change the course of action. There is thus plenty of scope for further research to establish whether the

[14] See also MG Porcedda, Cybersecurity and Privacy Rights in EU Law. Moving Beyond the Trade-off Model to appraise the Role of Technology (European University Institute 2017), ch 8; MG Porcedda, *Privacy by Design in EU law. Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection* (Lecture Notes in Computer Science, 2018).

[15] Quoting C Reed, *Making Laws for Cyberspace* (Oxford, Oxford University Press, 2012).

triad could, with the right conditions in place, find a different default mode of co-existence, especially in light of upcoming legislation on data flows and streamlining automation.[16]

II. Research trajectories and the future of the triad

To quote Brenner, 'it is much easier to criticize an existing system of [cyber] threat control than it is to develop a viable, effective alternative'.[17] This is especially the case at times of transition. While the search for new constitutional ways to deal with the digital unfold,[18] the pandemic and return of war in Europe may lend support to challenges to the neoliberal order.[19] We may be witnessing the waning of such an order and the waxing of contending alternatives. Some historical depth can help identifying root causes and areas for priority intervention.

The legal recognition of privacy emerged together with the evolution of modern technology in the nineteenth century and authoritarian regimes of the first half of the twentieth century. Both cybersecurity and data protection emerged with computing in the second half of the twentieth century, in a bipolar world order in which the fight over technological innovation was one of the many grounds on which the Cold War was contested. In both cases, the desire to innovate to serve defence, research, trade, or all of these at once prevailed over precautionary approaches. '*Laissez innover*',[20] couched for data flows as '*laissez processer*', has permeated first research, then the market and subsequently

[16] Eg, European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (Communication) COM(2020) 842 final 2020/0374 (COD)'; Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1; European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (AI Act) and amending certain Union legislative acts (Communication) COM(2021) 206 final 2021/0106 (COD), (2021).

[17] Brenner (n 12) 167.

[18] Eg, under the banner of 'code is law' and digital constitutionalism, see ch 5, section IV.

[19] For a pre-pandemic critique of commercialisation: L Newlove-Eriksson et al. 'The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security' *The International Spectator* (2018) 53(2) 124-140.

[20] J McDermott, 'A Special Supplement: Technology – the opiate of the intellectuals' *The New York Review*.

legislation. The neoliberal, new managerial turn that ushered in multi-stakeholderism and co-decision-making[21] gave the market an increasingly big say on regulation.

Such processes are deeply embedded in the fabric of EU law. Member States were utterly aware of the promises and challenges inherent in computing and data processing – in addition to longstanding privacy issues – as early as the 1960s. The European Commission pointed to the tech gap affecting Member States and potential interventions in the area,[22] but the times were politically unripe for joint action. Member States were protective of their monopolies and potentially in competition with one another in areas in which they had not given up sovereignty. In the words of former high-level EU official Heinrich Von Moltke, 'one tried to keep the best for oneself, even if it meant collaborating with US or Japanese corporations if necessary'.[23] Ironically, the EU could only become the norm-setter for privacy and data protection after the triumph of neoliberal capitalism, the end of the Cold War, the Treaty of Maastricht and the breaking of telecommunication monopolies. The same cannot be said for cybersecurity, possibly on account of its strong connection to traditional state functions that have not been transferred (yet?) to the EU.

The starting point is to see whether EU law – or any other jurisdiction – can withstand radical shifts, by questioning the overt goals and investigating the unintended effects of regulatory strategies, such as the effacement of technology from the law.[24] Regulatory strategies originally serving the de-politicisation of technology[25] for the sake of

[21] See generally S Borrás and J Edler (eds), *The Governance of Socio-Technical Systems. Explaining Change* (Cheltenham, Edward Elgar, 2014); H Wallace, MA Pollack et al. (eds), *Policy-making in the European Union* (Oxford, Oxford University Press, 2014).

[22] Council of the European Union, Ministers of the Common Market, 'Resolution of the Science Ministers of the Common Market calling Maréchal group to investigate EU cooperation in 7 fields, including data processing and telecommunications – Luxembourg Resolution (October 1967)'; Commission of the European Communities, European Society Faced with the Challenge of Information Technologies: a Community Response, COM(79) 650 final, (1979).

[23] '...on a essayé de garder le meilleur pour soi-même, quitte, le cas échéant, à coopérer avec des firmes japonaises ou américaines.' HV Moltke, *Interview with Moltke, Heinrich Von. The European Commission 1958-1973. Memories of an Institution* (2004).

[24] A similar investigation could be done for the organised and serious crime logics that characterise the approach to the AFSJ.

[25] Nau (n 13); J Kronlund, *Integration through depoliticization: how a common technology policy was established in the EU.* (CORE (Copenhagen Research Project on European Integration) Working Paper, 1995); C

regulating it may now be favouring unbridled technological change instead. Technology neutrality can be made to exploit the law's mandate to be of universal application to serve market interests, interests advanced by the market thanks to its monopoly of innovation. 'Technology effacement' serves innovation, but what is innovation and just how fundamental is it? Is it an end in itself or a trope to evade legal constraints? And if it is the latter, is it worth it? The prioritisation of innovation, combined with the normalisation of technological change, has made it impossible for the law to keep up with the pace of technology. But even when the law catches up, the market appropriation of law making corrodes the RoL from within. In agreement with Cohen, the law has evolved to meet the new economic demands; Cohen's invitation to consider the need for a RoL 2.0 is compelling.[26] This includes reconsidering 'slower, more atomistic, and more court-centered'[27] approaches.

Against this background, the current application of RoL-based proportionality enriched by the essence of the right may end up damaging rather than protecting rights. How exactly can the essence of the right to data protection be a fail-safe against powerful interests, when it is those powerful interests that determine the threshold for the essence? The example here is that of measures to safeguard the integrity and confidentiality of data, the significance of which is tied to standards. There is, at a minimum, the need to discuss how the essence works in a co-decision environment, whether it is a missed opportunity, and whether it could possibly backfire against rights holders.

This research focussed on the EU law in force at the time of writing. Important legislation affecting data flows and streamlining automation, which will soon enter into force or is in under discussion as part of the EU strategy for cybersecurity, for data and the digital agendas,[28] may reinforce or alter the dynamics described in these pages, for instance

Colini and ED Pino, 'National and european patterns of public administration and governance' in Magone (ed), *Routledge Handbook of European Politics* (London, Routledge 2015).

[26] JE Cohen, *Between Truth and Power* (Oxford, Oxford University Press, 2019) introduction and ch 7.

[27] ibid, conclusions.

[28] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'The EU's Cybersecurity Strategy for the Digital Decade' (Joint Communication) JOIN (2020) 18 final;

by attributing legal personhood to technology,[29] making the conversation more pressing. The inclusion of the national implementation of EU law, including national case law, could point to a greater protection of rights, thanks to the availability of more tools drawn from Member States' *ordre public*.

Ultimately a change of course would have an impact on much more than the triad. At stake are not just cybersecurity, privacy and data protection, but the survival of democratic orders and the flourishing of human nature as we know it.

European Commission, 'A European Strategy for Data' (Communication) COM (2020) 66 final; European Commission, 'A Europe fit for digital age. Shaping Europe's digital future' (Communication) COM (2020) 67 final; European Commission, '2030 Digital Compass: the European way for the Digital Decade' (Communication) COM (2021) 118 final

[29] Hildebrandt, M, Law for Computer Scientists and Other Folk (Oxford, Oxford University Press 2020), ch 9.