Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

SCHOOL OF LAW

LEGAL STUDIES RESEARCH PAPER SERIES

PAPER NO. 16/2023

December 2023

[The Effacement of Information Technology from EU Law: The Need for Collaborative Approaches to Redesign the EU's Regulatory Architecture]

[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/

The Effacement of Information Technology from EU Law: The Need for Collaborative Approaches to Redesign the EU's Regulatory Architecture

Maria Grazia Porcedda[1]

[This is a draft article drawing from a keynote speech delivered at the 18th IFIP Summer School on Privacy and Identity Management, University of Oslo, and forthcoming in F. Bieker, S. De Conca, I. Schiering, N. Gruschka. M. Jensen, Proceedings of the 18th IFIP Summer School 2023, Advances in Information and Communication Technology. Please only cite the version of record (published version).]

Abstract: *EU information technology law is built like a multi-storey house: on the ground floor is technology development and on the top floor are regulatory principles and rights; in the middle floor lie standards, which should connect the top with the ground floor. The house is built on the premise that these floors are seamlessly connected, but are they? The multi-storey house was in fact built without staircases, causing a practical disconnect between regulatory principles and technology development. This keynote speech, which draws from the 2023 book 'Cybersecurity, Privacy and Data Protection in EU law' (Hart Publishing 2023), will explore why information technology is effaced from EU law in practice, and the implications for cybersecurity, data protection, data markets, identity management, privacy and many other fields. This keynote speech will explore what collaborative approaches may be needed to redesign the EU regulatory architecture.*

Keywords: cybersecurity, privacy, data protection, EU law, information technology, Barbenheimer, Barbie, Oppenheimer

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

1 The research question: from identity to privacy, data protection & cybersecurity

Good afternoon, it is a great pleasure to be presenting at the 18th IFIP summer school. The title of my keynote is 'The effacement of information technology from EU law: the need for collaborative approaches to redesign the EU's regulatory architecture'. In this keynote, which stems from my recently published book,[2] I will invite you to reflect on one trait of European Union (hereafter EU) technology law, which I call the effacement of information technology from EU law. I will first retrace the steps of my research question, introduce cybersecurity, privacy and data protection from a legal perspective and then focus on the effacement of information technology from the law.

The interplay of cybersecurity, privacy and data protection is not the focus of this keynote, but I will use it as a springboard for illustrating the key points. The research question sets the background to what is to come: it draws the research trajectory and helps us framing academic work as dynamic work-in-progress. My research question began with questions about identity formation: who decides what we are? What mechanisms support and interfere with the carving of our own selves? For personal reasons, I was particularly interested in conformism and surveillance mechanisms, and since these reflections happened in the decade that followed the 9/11 attacks and the war on terror, I was especially drawn to the 'security v liberty' debate, where the usual victims were privacy and data protection, which are important mechanisms in support of autonomy and identity formation. After visiting the Silicon Valley and doing legal research on cloud computing, I started considering the possibility that cybersecurity disprove the 'security v liberties' debate. So here is how my journey began. The question I worked on was 'how can we reconcile cybersecurity with privacy and data protection in EU law'? Before I address this question, I would like to invite you to take advantage of this summer school to engage in storytelling on your research question, as a very powerful mechanism to understand your motivations in research and what may help you to find answers. I hope to hear from you in the coming days.

[2] Maria Grazia Porcedda, 'Cybersecurity, Privacy and Data Protection in EU law. A law, policy and technology analysis (Hart Publishing 2023).

2 The interplay between cybersecurity, privacy & data protection in EU law

Back to the research question, which we will use to inductively introduce the effacement of technology from EU law, you may all be familiar with cybersecurity, privacy and data protection, but you may not all be familiar with their position in law. EU law works hierarchically: constitutions and charters of rights have greater strength or force and trump lower sources such as secondary law and soft law. In EU law, privacy and data protection are currently hierarchically higher than cybersecurity. They are rights, which are supposed to have a core that cannot be violated (Article 52(1) CFR),[3] and data protection is also found in the Lisbon Treaty[4] (Articles 39 TEU and 16 TFEU). They are implemented by secondary law, such as the all-familiar General Data Protection Regulation.[5] Cybersecurity currently lacks explicit primary law grounding and is a policy area given substance by secondary law.

[3] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 (CFR).
[4] Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), OJ C 83/01 (Lisbon Treaty).
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Gen-eral Data Protection Regulation) [2016] OJ L119/1.

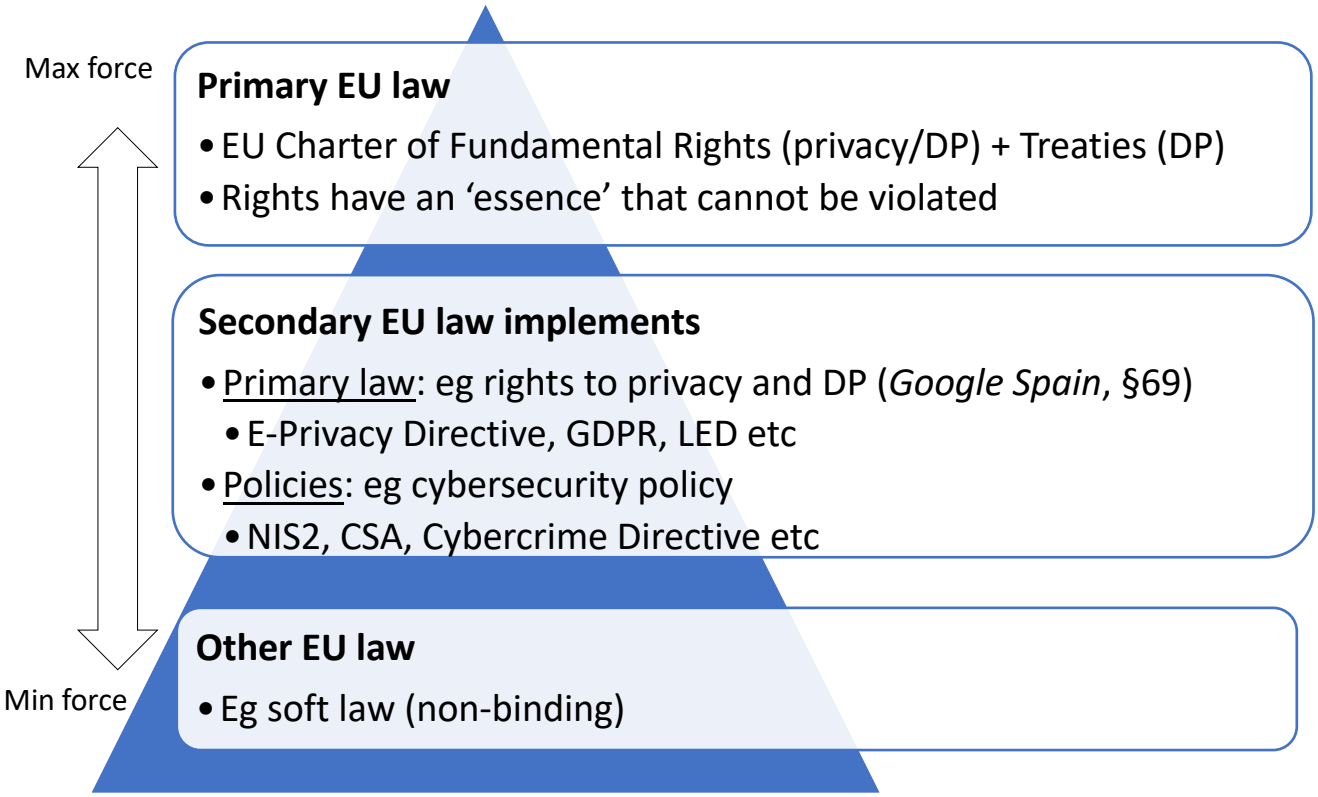


Figure 1 Relative force of cybersecurity, privacy and data protection in EU Law

Let us take a closer look at these terms. Following Article 7 CFR, the right to privacy means that 'Everyone has the right to respect for his or her private and family life, home and communications'. Following Article 8 CFR, the right to data protection means that 'Everyone has the right to the protection of personal data concerning him or her.' Limitations placed on these rights must respect the rights' essence (Article 52(1) CFR). However, the Charter does not list what such an essence may be, which is for Courts to identify, as they interpret the law. The Court of Justice of the European Union (hereafter CJEU) has thus far identified two relevant notions of the essence for the right to privacy and data protection. For privacy, these are the content of communications [often couched in terms of **confidentiality**][6] and 'the [revelation of] very specific information concerning the private life of a person'.[7] For data protection, it is the provision in the legal basis of security safeguards (**integrity** and **confidentiality**) and purpose limitation. [8] Note the words in bold: integrity and confidentiality.

[6] Digital Rights Ireland and Seitlinger and Others, Joined cases C-293/12 and C-594/12, EU:C:2014:238, para 39.
[7] Opinion 1/15 of 26 July 2017 pursuant to Article 218(11) TFEU EU:C:2017:592, para 150
[8] Opinion 1/15 of 26 July 2017 pursuant to Article 218(11) TFEU EU:C:2017:592, para 150

What about cybersecurity? We find a definition in Article 2.1 of the Cybersecurity Act, [9] which reads «Activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats». This is a very broad definition: cybersecurity embraces widely different fields, ranging from network and information systems security to cybercrime prevention, the collection of e-evidence, cyberpeace and the prevention of cyberwar. This is a huge field compared to what was the original narrow understanding of cybersecurity as network and information security (hereafter NIS), defined in Article 2.3 of the Cybersecurity Act as 'the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services …». Note again the use of confidentiality and integrity.

We have picked up some common terms: confidentiality and integrity. One of the avenues I explored in my work to answer the research question was to leverage these principles, which are common to information security, privacy engineering, and the law of data protection, to see whether they could help us identifying a way for these three interests to be reconciled. We can create tables of equivalences, which should help us achieving technical and operational measures that align with cybersecurity, privacy and data protection embedded in risk management (discussed further below). To build such equivalences, I drew from privacy engineers work on protection goals and security properties, understood as a principle or feature that characterises the achievement of the security/privacy objective.[10] The flipside to goals or properties are threats. Design strategies are blueprints for achieving the goals or maintaining the property and avoiding the threat. The table shows the example of integrity as the 'property that data has not been altered or destroyed in an unauthorised manner', which is the flipside to tampering and could be met

[9] 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 or CSA) [2019] OJ L 151/15.
[10] Kim Wuyts, INDDUN: a Privacy Threat Analysis Framework; George Danezis et al.: Privacy and Data Protection by Design – from Policy to Engineering (ENISA, 2014); Jaap-Henk Hoepman, Privacy by Design Strategies (The Little Blue Book) (2022).

with the design strategy 'control'. I then connected these notions to the legal bricks of privacy and data protection: the components

of rights, the essence, legal principles and specific provisions of secondary law. Examples of how this may look for privacy and data protection are contained in the excerpts of tables below.[11] However, I will not devote time to these tables, as they deviate from the main objective of this talk.

	Essential component	Essence (CJEU)	Protection goal (PG) & security property (SP)	Design strategy (DSs)
Private life		Revelation of very specific information concerning the private life of a person (not limited to certain aspects)	Confidentiality (PG/SP) Authorisation (SP) Authentication (SP) Unlinkability (PG)	Hide Aggregate, minimise, separate
	i. Physical & psychological integrity			

Art 8		Essential component	Essence (CJEU)	GDPR Principle (& FIP)	Protection goals (PGs)	Design strategy	Security property (SPs)
Paragraph 1	Protection	**The whole architecture of data protection** **ToMs: Security** **Subsumed ToM minimisation**	confidentiality & integrity	Integrity and confidentiality FIP security	**Confidentiality** **Availability,** **Integrity** Intervenability	Hide Control Minimise	**Availability** Authentication and non-repudiation (organisational measures) **Confidentiality** **Integrity**
				Data minimisation FIP collecting limitation	Unlinkability Transparency		Integrity Utility

At first (especially at PhD level, where I focused on NIS rather than cybersecurity as intended now) it seemed I had cracked the cybersecurity, privacy and data protection problem. But is it so? Think about what 'confidentiality' means in your academic discipline/field and the main sources/mechanisms used to define confidentiality. Is this a technical process and how does this affect technology? Or is this a legal process, and how does this affect technology?

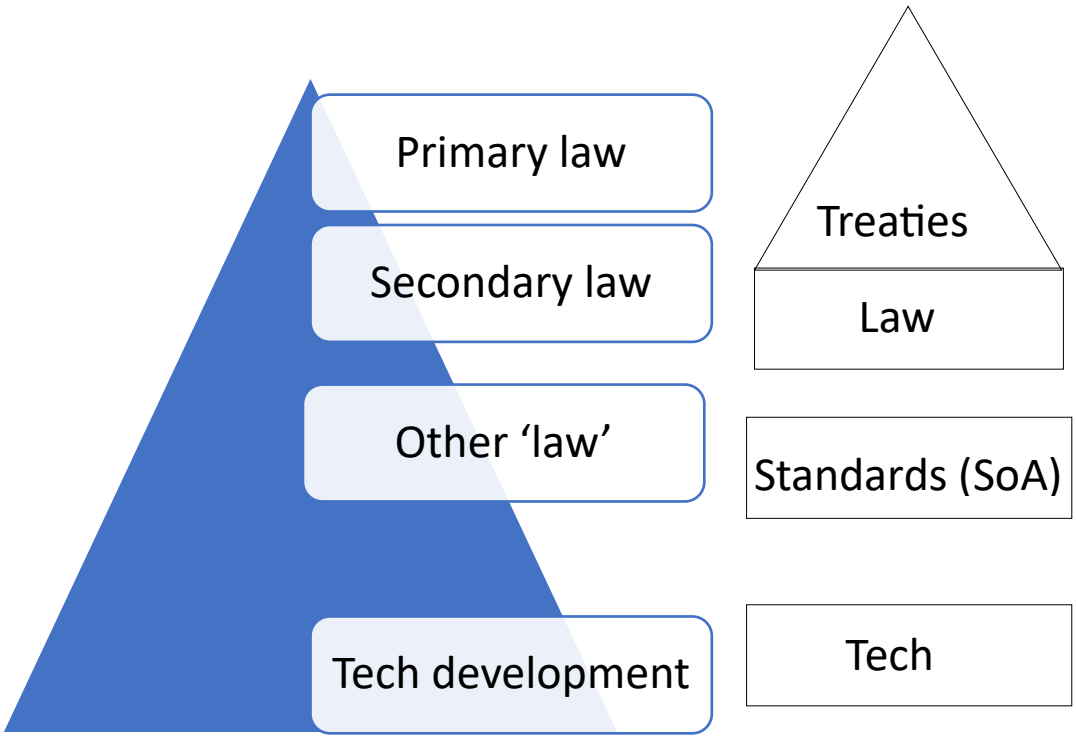
[11] Porcedda (2023, 94 and 125 (n 2).

The answer to these questions is that confidentiality does not mean to computer science and software engineering what it means to law and is overseen by different processes in the two disciplines. Such differences carry implications both for cybersecurity, privacy and data protection and for technology law more generally. They are very important when we look at the architecture of cybersecurity, privacy and data protection in EU law and feed the effacement of technology from the law. Which is what we will focus on in the following, with the help of the cinematic event of 2023 – 'Barbenheimer' – it is the summer after all!

3 The effacement of information technology from EU law (up to 2022) – lessons from Barbenheimer

Earlier on we saw the legal pyramid, a metaphor for the traditional hierarchy of legal sources, where primary law sits at the hierarchical top, secondary law is immediately below, followed by other forms of law lower in the hierarchy; these include 'soft law' such as standards. Technology design, although not formally 'law' per se, thanks to Laurence Lessig who wrote the famous book 'Code' in 1999,[12] (building on Reidenberg's Lex Informatica[13]), exert regulatory power, which is shown here at the bottom of the pyramid. Whether code embodies the lowest form of legal force is open to debate, but we will leave this debate for today.

[12] Lessig, L: Code: And Other Laws of Cyberspace. Version 2.0 (New York, Basic Books, 2006).
[13] 13. Reidenberg, JR: Lex Informatica: the Formulation of Information Policy Rules Through Technology (1998) 76 Texas Law Review 3



Here is where the first Barbenheimer reference comes into play. Barbie's house in Barbieland also has three floors that not just happen to match the layers of the pyramid but also help us explaining how the law hopes to influence standards and then technology design: the house has no staircase, but luckily Barbie musters the forces of the universe to gracefully flow from top to bottom (or slide down from the terrace to the pool). EU technology law similarly lacks direct mechanisms for influencing information technology standards and design, hoping instead to 'magically' flow from top to bottom.

Why is this as such? Here Oppenheimer comes to the rescue. The legal framework we have is a reflection of the post WW-II world order influenced by competition over scientific innovation justified by Cold and post-Cold War efforts. Nations tried to support – or curb – innovation by using standardization and this is what the EU did to build the Single Market for products and services. In line with the prevailing political economic doctrines (Reaganomics, liberalisation) of the 1980s that aimed to limit governmental interference, technology neutrality was introduced to boost innovation: the legislator should not choose nor ban a specific technological solution, provided it meets the benchmark, typically set by a standard, which in

the EU New Legislative Framework carried legal force.[14] Crucially, however, in the unbounded days that followed the end of the Cold War, software was excluded from the interpretation of product and the New Legislative Framework did not apply to it. Regulation brought in to deal with data flows and information technologies other than products (software) included technology neutrality without mechanism to select standards, which were left to the market. We may say that a permissive approach prevailed over other, potentially more precautionary, approaches. The impact of such approaches was initially limited by sectoral regulation, but digitization, smartphones, cloud computing and sensors (among others) have blurred the boundaries between sectors meaning that these approaches are now pervasive across information technology and data flows.

What about information technology and data flows? Matters such as information security and data flows were initially overseen by 'soft' principles. In some fields however, such as data protection, it became clear that principles were too weak on their own and were wrapped in 'hard' legislation, such as Treaties and secondary law. Most of us may know the history of data protection, where the challenges of digitization made it clear that extra steps in the form of privacy enhancing technologies (hereafter PETs) were needed, and which led to calls for increasingly harder regulation incorporating legal devices drawn from many traditions, such as 'by design' approaches usually credited to former Ontario Information Commissioner Ann Cavoukian. 'By design' has found its way into Article 25 GDPR as well as in cybersecurity legislation. But how is this supposed to work? In spite of much ado, the GDPR does not contain a list of PETs (which are not even mentioned) and offers very limited suggestions as to what 'by design' might mean. In the architecture of the GDPR, the expectation is that data controllers or operators of essential services in old NIS parlance will be able to pick the best 'by design' options because the market will have delivered them.

The parallel with Barbie is irresistible; in Barbieland there's the conviction that the negative effects of Barbies – pushing for a stereotypical and traditional model of womanhood – was

[14] This is discussed in-depth in Porcedda (2023), 148–50, 152 and 154 (n 2).

addressed with the introduction of career Barbies. Since Barbies can be what they want, sure feminism has won! Since we have Art 25 GDPR (and equivalents in NIS legislation), sure by design will happen!

But can the market deliver? My answer is, currently no. We need to look at how the architecture of technology law works in practice. Remember, the law works on the basis of technology neutrality, meaning that the law neither chooses nor bans the technologies that could implement it. Many instruments, especially in the area of security, mention generic tools, so the law does 'tooling'. Pay close attention: the law in force up to summer of 2022 does not address technology developers; there are no obligations for technology developers who are not data controllers to build technology according to the desired regulatory principles (only incentives for processors). The obligation to choose technologies that comply by design with principles embedded in the law rests on technology users, such as data controllers, operators of essential services etc. How do users choose among the existing options? The expectations is that they do so through 'the state of the art' – whatever is the most advanced technologies at hand. However, there is no catalogue for the state of the art, so who decides? The market does, based on standardization. Who writes standards? The market does, and some governments, through international processes where Big Tech plays an important role, and which have been heavily criticised in light of its composition (perhaps these mechanisms are similar to kendom?). Standardisation relies on certification, which is part of national private law, thus far outside the remit of EU law, so there's room for great disparity. In essence, EU tech law does all but moulding technology, which becomes effaced from EU law in a dangerous game of pass the parcel.

At the end of the line there are European judges, and you may think this is where the parcel stops, but unfortunately it does not. Judges are tasked with interpreting the law and are cautious not to engage in judicial activism, in the sense that they do not wish to substitute themselves to parliaments. So, if the law does not address technology, it is unlikely the judges will. And indeed, the EU cases where judges engage with concrete technologies are few and sparse. The classic case-by-case approach means that judges fail to appreciate the impact of the same technological solutions across sectors, the classic example being that of the same monitoring technologies applied across different fields. It also means that the

essence of rights becomes market-driven.[15] If neither the law nor judges addresses actual technologies, we are confronted with a technology 'indeterminacy loop' in the law.

Far from infusing technology with the desired principles as if by magic, technology law falls in the void, much like Barbie does when, having awakened, falls from the rooftop of her house. How can the PET market flourish against this background? Before concluding I would like to say a word about risk, which some may think has been overlooked. Risk management is the task of businesses and responds to logics vastly different from those of proportionality which govern legislation; I'll defer to the excellent work of Raphael Gellert[16] on this point. But risk management without PETs and real by design solutions ends up being a box-ticking exercise.

So, the EU regulatory architecture has, consciously or unconsciously, effaced technology from the law. Recent legal initiatives are taking cybersecurity and Artificial Intelligence under the legislative umbrella of the New Legislative Framework, the framework used to build the Single Market and which gives legal value to standardization. I am however not persuaded yet this will address the problem. First of all, we have built all of cyberspace outside of the New Legislative Framework – are we closing the stables' door after the horses have escaped? Secondly, we need to have a serious conversation about who drives standardization. Are recent efforts to redress representation working? It's interesting to know that in a 2022 case the CJEU did not take issue with the control exercised by industry in the elaboration of standards.[17] And whose standards are going to prevail? Will they be the US standards – some says the NIS mirrors NIST frameworks?[18] Will it be Chinese? Or European? Or will there be a standards' war?[19] The same fragmentation that exists in the legal framework is likely to be replicated for standards, but could possibly be ten time worst. Finally, standards rely on ontologies that are not necessarily aligned with legal/judicial principles. How do we come out of this? I believe we need to pool our disciplines to find

[15] This mechanism is discussed in-depth in Porcedda (2023), 193, 258-59, 262-69.
[16] Gellert, R: The Risk-Based Approach to Data Protection (Oxford, Oxford University Press, 2020).
[17] Stichting Rookpreventie Jeugd and others, C-160/20, EU:C:2022:101
[18] Shackelford, SJ, Russell, S and Haut, J: Bottoms up: A Comparison of Voluntary Cybersecurity Frameworks (2020) 16 UC Davis Business Law Journal 217–260.
[19] Peng, S Y: 'Private' Cybersecurity Standards? Cyberspace Governance, Multistakeholderism and the (ir)relevace of the TBT Regime' (2018) 15 Cornell International Law Journal.

solutions. We need to find solutions that take into account how case law, technology design, economic incentives, management practices, ontologies, regulatory approaches and the protection of rights work. For this, we need serious interdisciplinary cooperation - consider this an open invitation. Thank you very much for your attention!