The CDSL Working Paper Series

WP7/2024

CYBER & DATA SECURITY LAB

Data privacy law as a new field of law

Vagelis Papakonstantinou

CDSL Working Papers have been drafted by CDSL researchers and are made available via the CDSL website in order to promote academic exchange and discussion. They do not warrant fitness for any purpose and their contents should be treated at all times as work in progress.

Reference to a CDSL WP should be made as follows: [*Vagelis Papakonstantinou*] [Data privacy law as a new field of law], CDSL Working Paper [7/2024], available at https://cdsl.research.vub.be/en/workingpapers

Abstract

The turn of the 1980s was a milestone period in the development of data privacy laws, that was only paralleled by the turn of the 2020s. The former saw the introduction of Convention 108 by the Council of Europe in 1981 and, four months earlier, the OECD's Guidelines "governing the Protection of Privacy and Transborder Flows of Personal Data". Apart from the above two international instruments within only a few years' period France, Germany and the United Kingdom all introduced personal data protection legislation within their respective jurisdictions. the same milestone period for the development of data privacy laws has been witnessed around the turn of the 2020s: In the EU the General Data Protection Regulation and the Data Protection Law Enforcement Directive came into effect in 2018; the Council of Europe's Convention 108 was modernised also in 2018. In the USA, California's Consumer Privacy Act was introduced in 2018; China introduced its own relevant legislation in 2021; Brazil and India acquired their first relevant law in 2020 and 2021 respectively. In Europe, a GDPR mimesis phenomenon was noted. Forty years after its firm establishment, data privacy law is reaching its maturity point and international renown. In view of the above, can there perhaps be talk of a new legal field? Have data privacy laws over the past forty years formulated a separate field of law? Or are we simply dealing with important but solitary, standalone pieces of legislation? If a new legal field has indeed been formed, how will it be called? "Data protection law", "privacy law" or a combination of the two? However, perhaps more pertinently, do these distinctions matter at all? What is a "field of law" within Roman and Common Law legal systems and what is the significance of its continued existence? What are the criteria for its designation? Does this distinction bring any concrete and practical benefits to law today? If yes, and if legal field status was actually acknowledged to data privacy law, what would these be? The analysis that follows aims at addressing these questions.

Table of Contents

1.Introduction 4

1.1 A point on terminology: “Data protection law”, “personal data protection law” or “data privacy law”? 6

1.2. EU’s preference for the term “data protection” may be in need of re-assessment 7

1.3. Data protection and privacy, a difficult, if not impossible, to break bond even under EU law? 10

1.4. The Council of Europe’s careful but unmistakable mixing of personal data protection and privacy 13

1.5. The international approach: Clear prevalence of “privacy”, as in “data privacy” or “information(al) privacy” 15

1.6. Conclusion: “Data Privacy Law” to designate both personal data protection laws and privacy laws in the digital 16

2. Formulation of a “field of law”: Importance and criteria 19

2.1. Legal taxonomy in Common Law systems 20

2.2. The Roman Law tradition of codes and legal fields 23

2.3. Conclusion: Criteria (and justification) for identification of a new legal field 26

3. Is data privacy law a new field of law? Applying the *data privacy law acquis* onto the legal field criteria 28

3.1. Commonality 30

3.2. Systemic distinctiveness 31

3.3. Public perception 33

3.4. Transcendence 34

3.5. Data privacy law as a legal field: Content and placement 35

3.6. The benefits of acknowledgement of legal field status for data privacy law 37

Conclusion 39

1.Introduction

The turn of the 1980s was a milestone period in the development of data privacy laws, that was only paralleled by the turn of the 2020s. The former saw the introduction of Convention 108[1] by the Council of Europe in 1981 and, four months earlier, the OECD's Guidelines "*governing the Protection of Privacy and Transborder Flows of Personal Data*".[2] Apart from the above two international instruments within only a few years' period France,[3] Germany[4] and the United Kingdom[5] all introduced personal data protection legislation within their respective jurisdictions. An initiative that started out in 1970 in the German state of Hesse[6] and was then followed in 1973 by Sweden[7] and in 1974 by the United States of America,[8] decidedly and forcefully entered the books of law.

Regardless of the introduction of the EU Data Protection Directive in 1995,[9] the same milestone period for the development of data privacy laws has been witnessed around the turn of the 2020s: In the EU the General Data Protection Regulation[10] and the Data Protection Law Enforcement Directive[11] came into effect in 2018; the Council of Europe's Convention 108 was modernised also in 2018.[12] In the USA, California's Consumer Privacy Act was introduced in 2018; China introduced its own relevant legislation in 2021; Brazil and India acquired their first relevant law in 2020

[1] ETS No.108, opened for signature on 28 January 1981.
[2] On 23 September 1980.
[3] Loi no 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 January 1978.
[4] Bundesdatenschutzgesetz (BDSG), 1 January 1978.
[5] UK Data Protection Act 1984.
[6] Hessisches Datenschutzgesetz, 7 October 1970.
[7] Data Act, 11 May 1973.
[8] The USA Privacy Act of 1974.
[9] 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 "EU 1995 Data Protection Directive").
[10] 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, p. 1–88 (the "GDPR").
[11] 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, p. 89–131, (the "LED").
[12] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 18 May 2018 (the "Convention 108+).

and 2021 respectively. In Europe, a *GDPR mimesis* phenomenon was noted.[13] Forty years after its firm establishment, data privacy law is reaching its maturity point and international renown.

In view of the above, can there perhaps be talk of a new legal field? Have data privacy laws over the past forty years formulated a separate field of law? Or are we simply dealing with important but solitary, standalone pieces of legislation? If a new legal field has indeed been formed, how will it be called? "Data protection law", "privacy law" or a combination of the two? Perhaps more pertinently, however, do these distinctions matter at all? What is a "field of law" within Roman and Common Law legal systems and what is the significance of its continued existence? Does this distinction bring any concrete and practical benefits to law today? If yes, and if legal field status was actually acknowledged to data privacy law, what would these be?

The analysis that follows aims at addressing these questions. First, attention will be given, under Section 1, to terminology: The focus will be turned to the EU and to the Council of Europe legal scene in order to demonstrate the need for "data protection" to be replaced by "personal data protection" and to highlight the inseparability of "personal data protection" and "privacy" before concluding that the new legal field would preferably be named "data privacy law". Subsequently, Section 2 will discuss the merits of a legal taxonomy in Common and Roman Law systems with the aim to identify these criteria (*commonality*, *systemic distinctiveness*, *public perception* and *transcendence*) that, if Common Law accepted the idea of a legal taxonomy, would serve to qualify a collection of laws as a legal field. Section 3 will assess whether data privacy law constitutes a new field of law through application of the above criteria onto a *data privacy law acquis*. Once existence of a new legal field has been established, its content and placement (within Roman legal systems) will be identified, classifying it within Constitutional Law and also considering personal data protection law a subfield of data privacy law. The Section ends highlighting the advantages that classification as a new legal field carries for data privacy law, by way of concrete benefits in its *form*, *interpretation* and *implementation*.

[13] Vagelis Papakonstantinou and Paul de Hert, *The Regulation of Digital Technologies in the EU: The law-making phenomena of act-ification, GDPR mimesis and EU law brutality*, Routledge, 2024.

1.1 A point on terminology: "Data protection law", "personal data protection law" or "data privacy law"?

Before discussing whether a new field of law has by now emerged on the protection of individuals with regard to the processing of personal data a note on terminology is considered necessary: The question would be, how would this new field of law be named? This is an important question both for general and case-specific reasons. As it will be seen under Section 2, any legal taxonomy is useful first and foremost as a tool for better organisation and understanding of the law. If this is to be accomplished, any acknowledged field of law needs to be characterized by a certain level of general understanding as to its exact contents: there can be little doubt to anybody what Intellectual Property Law or Competition Law or Environmental Law involves. Any confusion on terminology whereby, for example, certain legal scholars and practitioners would use the term "privacy" and its derivatives ("data privacy" or "information privacy") while others would use the term "data protection" would make designation of a new legal field on the same impossible.

This terminological problem is unique to the personal data processing field. While other fields of law have also strived recently for formal recognition (most prominently, Environmental Law, Medical Law or, even, Water Law), none had to struggle as early as to come up with a name commonly used by all its stakeholders. In fact, as aptly noted by Bennett and Raab, "*it is an almost ritual feature of any analysis on privacy to begin with a warning about the inherent difficulty, perhaps impossibility, of defining exactly what privacy is, and disaggregating its various dimensions*".[14]

[14] Colin Bennett and Charles Raab, *The Governance of Privacy : Policy Instruments in Global Perspective*, [2nd and updated ed.]. (Cambridge Mass.: MIT Press, 2006)., p.xxii.

1.2. EU's preference for the term "data protection" may be in need of re-assessment

Under EU law the term "*data protection*" has come to be used to refer to laws aimed at protecting individuals with regard to the processing of personal data. This is pronounced most prominently in the title itself of the "General Data Protection Regulation". The same is invariably the case in all EU legal theory and practice. For example, Directive 2016/680 is customarily referred to as the "Data Protection Law Enforcement Directive" or the LED;[15] Or, the public bodies entrusted with the monitoring of these laws' implementation are named "Data Protection Authorities" (DPAs) at Member State level and the "European Data Protection Supervisor" (EDPS) at EU level.

The use of the term "data protection" goes back several decades in European law-making history. Famously, the first data protection act was introduced in the German state of Hesse back in 1970:[16] It was there that for the first time the term "Datenschutz" was employed, a choice of words that was met with scepticism since its first appearance.[17] The reasons behind employment of this term are not entirely clear today. Despite however etymological difficulties,[18] this choice of words in German effectively dominated the laws that followed: Ten years later France got its first law on "*données à caractère personnel*" and Germany its first federal "*Bundesdatenschutzgesetz*". From then on it was only to be expected that the UK introduced its own "Data Protection Act" in 1984. By the end of the 1980s the term had been established all across Europe.

At this point it is important to note that apparently not everybody in Europe felt comfortable with this term. As its will be seen in section 1.3, the Council of Europe in 1981 named its own Convention on this matter "*Convention for the Protection of Individuals with Regard to the Processing of Personal Data*". More pertinently, however, for EU law purposes, the EU 1995 Data Protection Directive that preceded the GDPR was not formally named "data protection" Directive: Specifically, its name was "*Directive on the protection of individuals with regard to the processing of personal*

[15] See, for example, European Commission, COMM(2020) 263 final.
[16] See above, footnote nr. 6 .
[17] See Simitis S, Introduction, in Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenshutzgesetz, Nomos, 1978, p.53 with further bibliography dating back to 1971.
[18] Hondius claimed in 1980 that "*the expression "data protection," derived from the German Datenschutz, is.a term of art which, although etymologically incorrect, has been widely-accepted in Europe and elsewhere*" (Fritz Hondius, 'Data Law in Europe', *Stanford Journal of International Law* 16 (1980): 87., p.89).

data and on the free movement of such data". Similarly, nowhere in its text is the term "data protection" employed, with the exception of "data protection officials" that essentially translated the German term

"Datenschutzbeauftragte". Accordingly, the EU 1995 Data Protection Directive did not use anywhere in its text the term "Data Protection Authorities" and did not formally name its own working party as the "*Article 29 Working Party on Data Protection*",[19] but instead "*Working Party on the Protection of Individuals with regard to the Processing of Personal Data*". This cautious approach, steering away from explicit use of the term "data protection", was confirmed also in Article 16 TFEU, whose wording has been carefully formulated so as not to include this term in any of its provisions.

The basic problem with the term "data protection" is that it is implicit: The word "personal" is implied each time. In other words, the General Data Protection Regulation is not an EU Regulation aimed at protecting any and all data, but only personal data. Or, whenever Directive 2016/680 is referred to as the Data Protection Law Enforcement Directive (or LED) the word "personal" is implied in its title. Or, when the EDPS states that "*Regulation (EU) 2018/1725 lays down the data protection obligations for the EU institutions and bodies when they process personal data and develop new policies*" again the word "personal" is meant to accompany "data protection".[20]

Admittedly, implicit use of the word "personal" to accompany the term "data protection" was never a problem until recently in EU law, because there simply was no other way to interpret "data protection". Lack of any other EU legal instrument on the protection of "data" effectively meant that in the minds of all practitioners, stakeholders and parties concerned any "data" under EU law context were necessarily "personal".[21]

However, this is no longer the case. The first recent development in EU law that obscures the term "data protection" is the regulation of non-personal data by Regulation (EU) 2018/1807 "on a framework for the free flow of non-personal data in the European Union".[22] Acknowledgement of non-personal data means that "data" within EU law are no longer necessarily "personal"; It may well be the case that non-personal data are meant. Difficulties will soon increase, after all, once the European Commission's Data Governance Act[23] and Data Act will come into effect, diluting even further

[19] As self-named, see for example its Annual Reports.
[20] See the EDPS official website.
[21] The closest that the term "data" came to formal legal acknowledgement until recently was in the text of the 1996 EU Database Directive (Directive 96/9/EC) that actually refers to a "*database*" as a "*collection of independent works, data or other materials*". Things are, of course, expected to change once the DGA comes into effect.
[22] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018.
[23] COM(2020) 767 final, where "data" is defined as "*any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording*" (Art. 2.1).

the monopoly of the term "data" by personal data protection in EU law. **Consequently, out-of-context reference simply to "data" within EU law needs to be qualified each time by clarifying whether such data are personal or not.**

Difficulties occur in EU law also as regards the second component of the term "data protection", namely "protection":[24] "Protection" of any "data" in EU law until recently necessarily referred to the EU Data Protection Directive or its successor, the GDPR, in the absence of any other EU regulatory instrument with the same or similar subject-matter. Nevertheless, the situation has changed with the emergence of EU cybersecurity legislation, namely the Cybersecurity Act.[25] Since its release in 2019 "cybersecurity" in the EU means "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*" (Art. 2.1); "*Network and information systems*" mean, among others, the "*digital data stored, processed, retrieved or transmitted […] for the purposes of their operation, use, protection and maintenance*".[26] Consequently, cybersecurity under EU law is also aimed at the protection of data.[27] **In other words, under EU law today the term "data protection" is no longer monopolized by personal data protection legislation but could also refer to cybersecurity legislation.**

In view of the above the term "data protection" under current EU law can no longer be used to singularly identify the protection of personal data. It could also refer to the protection of non-personal data or even to network and information systems in the cybersecurity context. It has therefore become necessary by now to clarify, effectively using at all times the term "personal data protection" instead of only "data protection". In the same manner, the formal name of the GDPR or the informal name of the LED have proven presumptuous: Back in 2016 they may have been indeed the only players in EU law protecting any data, but circumstances have gravely changed within a few years' time. *Today, a more adequate naming of the GDPR would be "General Personal Data Protection Regulation" (GPDPR)*.

[24] See also Bygrave L, that felt the need to clarify that "*Data privacy is not fully commensurate with data security. This should be obvious from the above-listed principles but bears emphasis particularly since the European nomenclature for the field ('data protection') appears closely related to data security and has been conflated with the latter*" (Lee A. Bygrave, *Data Privacy Law: An International Perspective*, First edition (Oxford, United Kingdom: Oxford University Press, 2014)., p.2).

[25] 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.

[26] Art. 4.1(c), Directive 2016/1148.

[27] As also noted in German theory, see Kutzschbach G, IT-Sicherheitsrecht, in Hartmann Matthias, Medienrecht, Walter de Gruyter, 2011, p.262.

1.3. Data protection and privacy, a difficult, if not impossible, to break bond even under EU law?

Use of the term "data protection" to denote the protection of individuals with regard to processing of personal data was not a necessary development. At the same time when the Germans coined the term "Datenschutz" it was clear to everybody that the new legislation aimed at protecting individuals against the then emerging computers and information technology was intrinsically connected with the right to privacy.[28] In essence, outside Europe this realization culminated into the USA Privacy Act of 1974. **Of course, the relationship between personal data protection and privacy runs deep and is by now well-examined under European legal theory.[29] Nevertheless, clarity, if at all, exists only within EU law: As it will be seen in the subsections that follow, outside the confines of EU law (meaning, while still in Europe, and of course in any other part of the world) the bond between the two remains strong – if not unbreakable**.

Under EU law whatever confusion existed, or still exists, by the relationship between privacy and personal data protection was attempted to[30] be dispersed in the text of the Charter of Fundamental Rights, where the two were irreversibly separated in Articles 7 and 8 respectively. Specifically, Article 7 sets that "*everyone has the right to respect for his or her private and family life, home and communications*" while Article 8 sets that "*everyone has the right to the protection of personal data concerning him or her*" (par. 1). Accordingly, Article 16 TFEU, as seen above, was

[28] As most recently affirmed in the Handbook on European Data Protection Law (available for download by the EU Publications Office, version 2018, the "Handbook on European Data Protection Law"), p.18, but also a fact that was evident in all bibliography at the time and long thereafter, see, for example, Alan F. Westin and Michael A. Baker, *Databanks in a Free Society: Computers, Record Keeping and Privacy* (Times Books, 1972). Arthur Raphael Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press, 1971).Paul Sieghart, *Privacy and Computers* (London: Latimer New Dimensions, 1976). Hans Peter Bull, *Datenschutz, oder, Die Angst vor dem Computer* (München: Piper, 1984).; David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (UNC Press Books, 1989).and also OECD, The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, OECD Digital Economy Papers, No. 176, pp.7-9.

[29] Essentially concluding that "*data protection and privacy are twins, but not identical*" (De Hert P/Schreuders E, The Relevance of Convention 108, European Conference on Data Protection on Council of Europe Convention 108: Present and future, 2001; See also C Kuner, 'An International Legal Framework For Data Protection: Issues and Prospects', *Computer Law & Security Review* 25 (2009): 307–17.Maria Tzanou, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right', *International Data Privacy Law*, 2013.Lee A Bygrave, 'The Place of Privacy in Data Protection Law', *University of New South Wales Law Journal* 24 (2001): 277. Jan Holvast, 'History of Privacy', in *The History of Information Security: A Comprehensive Handbook*, ed. Karl de Leeuw and J. A. Bergstra (Amsterdam ; London: Elsevier, 2007). Raphael Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection', *Computer Law &Security Review (CLSR)* 29 (2013): 522–30, http://works.bepress.com/serge_gutwirth/107; Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order', *International and Comparative Law Quarterly* 63, no. 03 (2014): 569–97.

[30] The results of this attempt remain doubtful: See, for example, Hendrickx stating that "*there is a strong (and reinforcing) overlap between Article 8 and Article 7 CFREU*" (Frank Hendrickx, 'Article 8 - Protection of Personal Data', in *The Charter of Fundamental Rights of the European Union and the Employment Relation*, ed. Philip Dorssemont et al. (Hart Publishing, 2019).

introduced in the Lisbon Treaty. It was its second paragraph that led to the release of the GDPR[31] and, accordingly, the GDPR contains no reference to privacy whatsoever in its text. This comes in stark difference to its predecessor, the EU 1995 Data Protection Directive, that contained thirteen occurrences of the word, most notably in its objective: "*In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*" (Article 1.1).

Despite concise and persistent efforts at the highest EU level to clearly distinguish between privacy and personal data protection, even under EU law co-existence of the two seems inevitable. As noted by Gonzalez Fuster, "*it cannot be inferred that the EU right to the protection of personal data has been completely disconnected from the right to privacy in EU law. What needs to be stressed, in any case, is that the connection between EU personal data protection and privacy is contingent, and that it is not stable*".[32] Perhaps nowhere else is this more demonstrable than in the case of EU's ePrivacy legislation. Back in the 1990s it was believed that the general principles of the EU 1995 Data Protection Directive would be complemented by sector-specific legislation customized to each field's particular circumstances and needs.[33] While this approach never really took off within the EU, the electronic communications (then, telecommunications) sector indeed benefited from such an approach:[34] As a result, the ePrivacy Directive has accompanied the field from 1997[35] until today (soon to be replaced by the draft ePrivacy Regulation). Despite their explicit naming as privacy-regulating instruments, their relationship with data protection is unmissable and explicitly acknowledged in all relevant texts.[36] This relationship is still acknowledged today, in the text of the draft ePrivacy Regulation: "*The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as*

[31] See Recital 12 of the GDPR.
[32] Gloria González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series, volume 16 (Cham ; New York: Springer, 2014)., p.268.
[33] See Spiros Simitis, 'From the Market To the Polis: The EU Directive on the Protection of Personal Data', *Iowa Law Review* 80, no. 3 (1995): 445., p.467.
[34] See V Papakonstantinou and P. De Hert, 'The Amended EU Law on EPrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights', *The John Marshall Journal of Computer & Information Law* XXIX, no. 1 (Fall 2011): 101–47., pp.32ff.
[35] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, repealed in 2003 by 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), as amended in 2009 and still in effect today.
[36] For example, "*Directive 97/66/EC [...] translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector*" (Preamble 4 of Directive 2002/58/EC).

personal data".[37] The above demonstrate that even with the help of legal tools at the highest level, a clear separation between personal data protection and privacy is not fully achievable in practice.

Another field where EU law is faced with the inevitability of mixing data protection and privacy is international data transfers in the context of its personal data protection legislation ("*transfers of personal data to third countries or international organisations*").[38] Famously, any transfer of personal data from the EU to a third country or an international organisation may take place only where the European Commission has decided that these ensure an "*adequate*" level of protection.[39] Such "*adequate*" level of protection is to be assessed in terms of examining its respective country's or international organisation's "*legislation, data protection rules, professional rules and security measures*".[40] Which legislation would that be, however? If the EU was committed to its clear separation between privacy and data protection it would automatically refuse to assess any privacy-related legislation and ask only for specialized data protection legislation from third countries and international organisations. Nevertheless, this has not been the case. The Commission has, pragmatically, granted "*adequacy*" status to countries that demonstrably mix data protection and privacy into their respective laws.[41] It is these laws that the Commission examined and found "*adequate*", therefore indirectly and tacitly acknowledging itself that the two cannot be separated.

At any event, it is not only the formalistic distinction between data protection and privacy in EU law that suffers: Perhaps most pertinently in the context of fundamental human rights, the distinction is blurred also in the minds of Europeans. This is demonstrated, for example, in the Eurobarometer report of 2015, that preceded the EU data protection reform package, where the two are seamlessly mixed.[42] The same approach was confirmed several years later, in 2019, under a Eurobarometer report on the GDPR itself.[43] The two reports showcase what is empirically witnessed daily also in Europe: Notwithstanding the fine, almost imperceptible distinctions of EU law, privacy and data protection are intrinsically connected under a difficult, if not impossible, to break bond.

[37] Preamble 5 of the draft ePrivacy Regulation.
[38] See Chapter V of the GDPR, the LED and Regulation 1725/2018 respectively.
[39] See, indicatively, Article 45.1 of the GDPR.
[40] Article 45.2(a) of the GDPR.
[41] See subsection 1.4, in particular the cases of Israel and Canada.
[42] European Commission, Special Eurobarometer 431, Data Protection Report, June 2015.
[43] European Commission, Special Eurobarometer 487a, The General Data Protection Regulation, June 2019.

1.4. The Council of Europe's careful but unmistakable mixing of personal data protection and privacy

In spite of the EU's formal use of the term "data protection" to denote the protection of individuals with regard to the processing of personal data, the terminological issue remains far from resolved even in Europe. In Europe there are two, if not competing then complementary, systems for the protection of personal data in effect today: That of the EU and that of the Council of Europe. The Council of Europe's protective system is composed of two pillars that have each developed significantly and largely independently over the past decades: On the one hand, Article 8 of the ECHR and, on the other hand, Convention 108+. If the issue of the relationship between privacy and personal data protection is resolved both substantially and terminologically within the EU's legal system (under the clarifications in the preceding subchapter), this is far from being the case within that of the Council of Europe.

The ECHR does not include any reference to personal data protection in its text; A separate individual right to data protection, as is the case in the EU, is not explicitly acknowledged. A committee of experts reported to the Council in 1970 that the mechanisms and remedies offered by the ECHR provide inadequate solutions to personal data processing problems[44] and in 1978 a proposal was endorsed to incorporate a right to data protection in the ECHR, however the idea was abandoned in favour of specialized Resolutions that ultimately led to Convention 108.[45] Nevertheless, this has not stopped the ECtHR, that rules on violations of the ECHR's provisions, from issuing since the 1980s case law of tremendous importance in Europe in the field of personal data protection.[46] The Court has achieved this result through application of Article 8 of the ECHR, namely the right to privacy: "*All persons have the right to respect for their private and family life, their home and their correspondence*".[47] It is on the basis of this wording, in

[44] See Frits W. Hondius, 'A Decade of International Data Protection', *Netherlands International Law Review* 30, no. 02 (August 1983): 103, https://doi.org/10.1017/S0165070X00012298., p.92 and p.110.

[45] Committee of Ministers Resolution (74)29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector, Council of Europe (1974); Committee of Ministers Resolution (73)22 on the Protection of the Privacy of Individuals vis-i-vis Electronic Data Banks in the Private Sector, Council of Europe (1973).

[46] The relevant analysis in the Handbook on European Data Protection Law (pp.18-20) is most relevant in this regard, because the Handbook is the result of cooperation between the EU (through its Fundamental Rights Agency and the EDPS), the Council of Europe and the ECtHR. Accordingly, the Handbook includes numerous references to relevant ECtHR case law to each data protection basic principle and component, as known in the EU, seamlessly switching between the two courts (CJEU and ECtHR). See also Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembrourg: Constitualisation in Action', in *Reinventing Data Protection?*, ed. S Gutwirth et al. (Dordrecht: Springer Science, 2009), 3–44.

[47] See also Gonzalez-Fuster, who notes that "*the ECtHR has given to the wording of Article 8(1) of the ECHR a wide, generous interpretation*", with further references (González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. p.95)

particular expressly acknowledging the intrinsic bond between privacy and personal data protection,[48] that the ECtHR has issued detailed decisions on the processing of personal data, frequently reflecting structures and mechanisms employed in the EU legal system.[49]

Convention 108 was released in early 1981, under the title "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*". Its article 1 provides useful input for the purposes of this analysis: "*The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*". Consequently, the intrinsic relationship between privacy and data protection was expressly clarified under Convention 108's objective and scope. Hustinx noted in this regard that "*to be clear: the Convention's approach is not that processing of personal data should always be considered as an interference with the right to privacy, but rather that for the protection of privacy and other fundamental rights and freedoms, any processing of personal data must always observe certain legal conditions*".[50] Convention 108 remained in effect for a little less than forty years, constituting (after ratification) a binding legal instrument for its signatory states.

Convention 108 was modernised in 2018 and is by now Convention 108+. **Although Convention 108+ was drafted simultaneously with the EU's GDPR and the LED, meaning that the distinction between a right to privacy and a right to personal data protection in EU law was well-known to its drafters, it did not hesitate to refer again explicitly to privacy in its text, as prominently as in Article 1 on its "object and purpose"**: "*The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy*". This wording, while clarifying many aspects that the 1981 formulation left open, confirms and maintains the strong bond between the two rights for the years to come.

[48] See, for example, the Satamedia judgement where the Court stated that "*Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged*" (Satakunnan Markkinaporssi Oy And Satamedia Oy v. Finland, 27 June 2017).

[49] See, instead of all, the Court's Guide on Article 8 of the ECHR, as updated on 31 August 2018, particularly its Chapter II.C.c, Privacy – Data Protection; Also, Council of Europe, Data Protection Unit, Case Law of the ECtHR Concerning the Protection of Personal Data, T-PD(2018)15, an impressive analysis of no less than 300 pages.

[50] Hustinx P, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 15 September 2014, available at the EDPS website.

1.5. The international approach: Clear prevalence of "privacy", as in "data privacy" or "information(al) privacy"

Outside Europe there is clear, strong and persistent preference for the term "privacy", most likely alone or in its derivative forms of "data privacy" or even "information privacy", to denote legal instruments aimed at protecting individuals with regard to processing of personal data. For example, the OECD has issued its "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*" in 1980 and updated them, under the same name, in 2013; The UN has appointed a Special Rapporteur on the "*Right to Privacy*" in 2015; The Asia Pacific region has released the APEC "*Privacy Framework*"; The African Union Convention, while in name referring only to "personal data" specifically and repeatedly refers to the protection of privacy in its text;[51] Canada, Israel and New Zealand, a selection of countries having achieved adequacy status by the EU, all refer to either Privacy Acts and/or Privacy Commissioners or Authorities;[52] The USA has been consequent in its employment of the term privacy both back in 1974, in its Privacy Act, and at state level, as demonstrated in California through its Consumer Privacy Act. Accordingly, taking stock of the terminological difficulties, the UN merges the metrics of "*data protection and privacy legislation worldwide*" in its UN index. Almost complete unanimity in the combined use of "data protection" and "privacy" as soon as exiting EU law boundaries is demonstrable also in legal theory,[53] in international *fora*[54], as well as, (perhaps most importantly within the context of a basic human right) general public perception.[55]

[51] See, for example, its Article 8.1.
[52] See also Hiroshi Miyashita, 'The Evolving Concept of Data Privacy in Japanese Law', *International Data Privacy Law* 1, no. 4 (2011): 229–38, http://idpl.oxfordjournals.org/content/1/4/229.short.
[53] See, for example, G Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, 1 edition (Oxford, United Kingdom ; New York, NY: Oxford University Press, 2014). Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law*, 6th edition (New York: Wolters Kluwer, 2017).Bygrave, *Data Privacy Law*.Alex B. Makulilo, ed., *African Data Privacy Laws*, vol. 33, Law, Governance and Technology Series (Springer International Publishing, 2016). James B Rule and G Greenleaf, eds., *Global Privacy Protection: The First Generation* (Cheltenham, UK; Northampton, MA: Edward Elgar, 2010).Or, the International Data Privacy Law journal, published by Oxford University Press.
[54] See, instead of all, the International Conference of Data Protection and Privacy Commissioners (ICDPPC).
[55] See Wikipedia's entry on "information privacy" ("*information privacy, data privacy or data protection laws*"), Britannica ("Data Protection, species of privacy law"), accessed in Winter of 2021.

1.6. Conclusion: "Data Privacy Law" to designate both personal data protection laws and privacy laws in the digital

In view of the above a straightforward global solution for naming any new field of law that may have been formulated by now on the protection of individuals with regard to processing of personal data seems impossible to achieve. While within the EU "personal data protection law" would be the obvious choice (under the clarifications of subsection 1.2 above), it is unlikely that this term would ever meet global acceptance. To make things worse, it would also not be compatible with the Council of Europe approach, that persistently keeps privacy in the picture and is also binding upon the same (EU) countries. More importantly, however, even when used outside the EU "personal data protection" would never come to mean what is meant by it within the EU, meaning a different right, and therefore context, to privacy. **Under EU law the two are (ideally) separated; Outside EU law, even if still in Europe, the two remain intrinsically connected**. Even if EU legal mechanisms and theoretical constructs on personal data protection were exported to the rest of the world, it is most likely that they would come to be used in one way or another connected with the right to privacy.

This after all constitutes the global practice already. At the time of drafting this analysis according to the UN Index more than 130 countries around the world have enacted some kind of personal data protection acts, most of which, if not outwardly using the term "privacy" in their title, most likely mixing the two in their actual provisions. Greenleaf, who provides a global metric[56] in parallel to that provided by the UN, while estimating that "*for the past 46 years since 1973, countries around the world have enacted new data privacy laws at an average rate of 2.9 new countries per year, giving a total of 134 laws by April 2019*",[57] notes that "*the concept of 'data protection' (or 'data privacy', which is the term used in this book) is now relatively well defined as a set of 'data protection principles', which include an internationally accepted set of minimum principles plus additional principles which are evolving continually through national laws and international agreements*".[58] As seen in the previous subsection, the same is the case (in the sense of mixing data protection and privacy) with practically all international organisations active in the field: The Council of Europe, the OECD and the UN.

[56] Graham Greenleaf, 'Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority', *Privacy Laws & Business International Report* 133 (2015).
[57] Greenleaf G, *Countries with Data Privacy Laws – By Year 1973-2019* (May 10, 2019). Available at SSRN: https://ssrn.com/abstract=3386510.
[58] Greenleaf, *Asian Data Privacy Laws*.

Legal scholarship for most of its part has employed the term "data privacy" whenever outside EU legal borders. Bygrave clarifies that "*data privacy law specifically regulates all or most stages in the processing of certain kinds of data*", before going on to explain that "*data privacy (or data protection) is not fully commensurate with privacy, at least if the latter is defined in terms of non-interference, limited accessibility, or information control*".[59] Similarly, the editors of the International Data Privacy Law journal clarify that "*we will focus on the area of 'data privacy' (eg, 'data protection' in the sense of the European Data Protection Directive 95/46, or 'information privacy' in the sense of the APEC Privacy Framework)*".[60] As correctly identified, from a schematic point of view the notions of privacy and personal data protection coincide but not entirely. In essence, the notion of privacy includes more than personal data and, at the same time, not all personal data are private.[61] Nevertheless, while conceptually this is a valid distinction, its value is mostly theoretical: As regards its first part, the expression of privacy of any individual in the digital realm will unavoidably have to come in some tangible (data) format so as for it to be protected, and such tangible format will most likely be classifiable as "*personal data*" within the personal data protection law meaning.[62] Similarly, while indeed not all personal data are private, the fact remains that whenever personal data need to be protected and specialized personal data protection legislation is missing the right to privacy has invariably been employed to fill in the gap, as after all most prominently evidenced by the ECtHR itself.

In view of the above it would seem that the term "data privacy law" would be best suited to globally describe the field of law regulating personal data processing. As a derivative term from privacy, it would confirm the global perception that the protection of personal data and the protection of privacy are intrinsically connected. However, its "data" component would be used to denote a digital, or at least factual context, whereby "*spatial, bodily and perhaps psychological dimensions*"[63] of privacy would not fall within its scope. Also, "data" would be a term preferable to "information"[64] because, taking into account that "information" is connected to meaning, first, "data" is a more comprehensive term better suited in a digital world of ones and zeros, and, second, its neutral character, although

[59] Bygrave, *Data Privacy Law*. pages 1, 3 and introduction respectively.
[60] Kuner C et al, *Editorial*, International Data Privacy Law, Issue 1 Volume 1, 2011.
[61] As, famously, put by the EU Court of First Instance (now General Court) in Bavarian Lager, (Case T-194/04); See also Gellert and Gutwirth, 'The Legal Construction of Privacy and Data Protection'. p.529-530, with further bibliography.
[62] In the words of the GDPR, "*any information relating to an identified or identifiable natural person*", Article 4.1.
[63] Bygrave, *Data Privacy Law*.p.3.
[64] For the purposes of this analysis "information privacy" is treated as a synonym to "informational privacy" (on the latter, see, indicatively, Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA: MIT Press, 2008). p.6.

mundane, removes an unnecessary layer of interpretation in the sense that it does not make interpretation on whether a certain piece of data falls under the law or not necessary. [65]

[65] In the words of Bing, "*It is conventional to distinguish between 'data' and 'information'. In order for data to be transformed into information, it has to be received and understood by someone. As long as these two conditions are not fulfilled, the data remains a collection of characters and is not transformed into knowledge*" (Jon Bing, 'Information Law?', *Journal of Media Law and Practice*, 1981. However, Clarke believes that "information privacy" is preferrable because it is the more descriptive of the two terms (Clarke R, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, available at http://www.rogerclarke.com/DV/Intro.html). On the preference for the term "information privacy", however noting merely jurisdictional preference reasons, see also Mark Burdon, *Digital Data Collection and Information Privacy Law*, 1st ed. (Cambridge University Press, 2020), https://doi.org/10.1017/9781108283717. pp.101ff.

2. Formulation of a "field of law": Importance and criteria

While still on terminological grounds, the notion of a "legal field" needs to be examined next. Indeed, the main question of this analysis, whether by now a new field of law, "data privacy law", has been formed, may sound legalistic to most. It is therefore important to demonstrate the merits of acknowledging "legal field" status to a particular set of laws. In view of the fact that essentially this is a question on the merits of legal taxonomy, this being a vast subject that ultimately refers to the fundamentals of Common versus Roman (Civil) law,[66] the analysis that follows will simply highlight the two different approaches between these two systems of law and attempt to Identify the **criteria, wherever applicable, for identification of a legal field**, taking into account that the (new) field of law under examination has been and still is predominantly developing in Europe,[67] therefore within the Roman law tradition.

[66] For the purposes of this analysis the terms "Roman Law" and "Civil Law" will be used as synonyms, notwithstanding the fact that Civil Law systems should be further distinguished between Germanic (Germany, Austria, Switzerland) and French (France, Italy) Civil law systems (see, for example, Ugo Mattei, 'Three Patterns of Law: Taxonomy and Change in the World's Legal Systems', *The American Journal of Comparative Law* 45, no. 1 (1997): 5., p.42 with further references). Similarly, as regards Common Law, the point of Weiss, that "*England and the United States belong to the common-law system, but the common law is not "common" in all respects*" ought to be kept in mind, despite of the fact that for this analysis' purposes Common law systems will be treated uniformly (Gunther Weiss, 'The Enchantment of Codification in the Common-Law World', *The Yale Journal of International Law* 25 (2000): 435., p.527).

[67] See footnote nr. 29.

2.1. Legal taxonomy in Common Law systems

Perhaps the best reasoning why a taxonomy in law is important can be found exactly where it is most visibly missing, namely in Common Law systems. Because Common Law legal scholars never adopted the basic legal taxonomies that are embedded in Roman law systems, important legal scholarship has been developed analysing both the merits of introducing such a taxonomy and, should these be accepted, the criteria upon which to build it.

As regards the former, meaning the merits of a legal taxonomy, Birks, while writing on English Private Law, states that "*better understanding of the law depends upon a sound taxonomy of the law*" before going on to predict that, "*if scholars turn their back to the taxonomic debate, common law will dissolve into incoherence since information which cannot be sorted is not knowledge*".[68] Similarly, Sherwin claims that "*a comprehensive formal classification of law provides a vocabulary and grammar that can make law more accessible and understandable to those who must use and apply it*".[69] In the same context, Varuhas states that "*legal categorization is fundamental to full understanding of the law, rigorous and complete legal analysis and coherent and rational legal development*".[70] Aagard (while in fact examining the same question as this analysis for Environmental Law) finds that "*classification is inherent and fundamental to the operation of law. Justice requires consistency. Legal classifications enable consistency by designating categories of similar situations to which a common set of principles applies. The category assigned to a situation thus may determine how the law applies to the situation*".[71]

[68] Peter Birks, *English Private Law. Volume I.* (Oxford ; New York: Oxford University Press, 2000). p. li. However, Birks has been vividly criticised in Common Law theory, being described an "*academic jurist in the Roman law tradition*" and a "*Leibnizian*", see Duncan Sheehan and T. T. Arvind, 'Private Law Theory and Taxonomy: Reframing the Debate', *Legal Studies* 35, no. 3 (2015): 480.

[69] Emily Sherwin, 'Legal Positivism and the Taxonomy of Private Law', in *Structure and Justification in Private Law: Essays for Peter Birks*, ed. C. E. F. Rickett and Ross Grantham, Illustrated edition (Oxford ; Portland, Or: Hart Publishing, 2008).

[70] Jason NE Varuhas, 'Taxonomy and Public Law', in *The Unity of Public Law?: Doctrinal, Theoretical and Comparative Perspectives*, ed. Mark Elliott, Jason NE Varuhas, and Shona Wilson Stark (Oxford UK ; Portland, Oregon: Hart Publishing, 2018).

[71] Todd S Aagaard, 'Environmental Law as a Legal Field: An Inquiry in Legal Taxonomy', *Cornell Law Review* 95 (2010): 221., p.224 with further bibliography.

Nevertheless, such elusive benefits as "*better understanding*" of the law[72] could not possibly sound convincing to all. While Common Law legal scholars have carried out important work in this regard, it appears that all relevant research has been inconclusive, first, when distinguishing fields of Public[73] or Private Law[74], and, second, as to why a taxonomy is needed at all.[75] Famously, the "Law of the Horse" has been used to undermine similar efforts.[76] Apparently, Common Law fundamentals sit awkwardly with classifications that originate in Roman Law. In the same context, important work has been carried out on the topic of regulation,[77] however in this case the legal toolset (norm-setting provisions, regardless whether dispersed or organised into fields of law) is considered given.

Outside legal philosophy and general theory of law, however, Common Law scholars and practitioners seem at ease to identify new fields of law. It would appear that, if the question on whether to have a taxonomy is removed from the picture, then identification of the criteria on the basis of which to distinguish a new legal field would be easier. For example, Kosseff's criteria while defining cybersecurity law are formulated as follows: "*To form the definition, we must answer five fundamental questions that examine the underlying values that should shape our cybersecurity laws: (1) What are we securing?; (2) Where and whom are we securing?; (3) How are we securing?; (4) When are we securing?; and (5) Why are we securing?*".[78] In the field of Environmental Law, essentially while dealing with the same question as this analysis, Aagard finds that "*a field of law can be understood as arising through the interaction of four underlying constitutive dimensions: Factual context, policy trade-offs, values and interests, and legal doctrine. An organizational framework for a legal field can apply to any one or a combination of these constitutive dimensions*".[79]

[72] Siems was able to identify an additional benefit, that "*researchers may also analyse how such legal classifications are related to non-legal ones*" (Mathias M. Siems, 'Varieties of Legal Systems: Towards a New Global Taxonomy', *Journal of Institutional Economics* 12, no. 3 (2016): 579.
[73] See Varuhas, 'Taxonomy and Public Law'. and also Paul Craig's response in Craig P, Taxonomy and Public Law: A Response, Public Law (2019), available at https://ssrn.com/abstract=3245496
[74] Birks, *English Private Law. Volume I.*
[75] See Sheehan and Arvind, 'Private Law Theory and Taxonomy'.
[76] "*Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well*", Frank H Easterbrook, 'Cyberspace and the Law of the Horse', *The University of Chicago Legal Forum*, 1996, 11.
[77] By way of introduction into the theory of regulation see, for example, Robert Baldwin, Martin Cave, and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Second Edition (Oxford University Press, 2011). Accordingly, this analysis refers only to laws, in the meaning of legal acts and not to any other tools of regulation (that, unavoidably, if existence of a legal field was acknowledged, would have to follow the same categorization).
[78] J. Kosseff, 'Defining Cybersecurity Law', *Iowa Law Review* 103, no. 3 (2018): 985–1031.
[79] Aagaard, 'Environmental Law as a Legal Field: An Inquiry in Legal Taxonomy'., p.236 (with further bibliography on p.239).

An important source of criteria by which to distinguish a new field of law is legal education, namely, the recognition of subjects for inclusion in the curriculum of law schools.[80] Law schools have had a history of at least 150 years on how

best to organise law in order to teach it to their students; Identification of a new field of law to teach in classes forms an integral part of this work.[81] While the curriculum of law schools may seem at an endless loop with legal taxonomy (if legal taxonomy recognized a new field of law then law schools will teach it and vice versa) it does bring an important criterion to the fore: The perceptions of the profession.[82] Law schools provide legal professionals to society: If during their formative years these have been taught that a particular field of law exists, then lawyers, judges and other professionals in the field will continue believing in its continued existence, for example advertising it in their law firms or CVs. Conversely, if more and more lawyers advertise expertise in a new area of law, then law schools will be inclined to include it in their curricula. The above serve to demonstrate that the perception of the profession, regardless whether in academia or in practice, formulates a separate and important criterion in the designation of a new field of law.

[80] See Martin Levine, 'Four Visions of the Law School: Law and Aging As a New Legal Field', *Journal of Legal Education* 31 (1981): 424., p.439.
[81] In this context, Levine (ibid) identified four models of legal education that provide us with concrete criteria for designation of a new legal field.
[82] A practical application can be found at James J Fishman, 'The Emergence of Art Law', *Cleveland State Law Review* 26 (1977): 481.

2.2. The Roman Law tradition of codes and legal fields

Classification and distinction among fields of law is a predominantly legal trait in Europe, where Roman Law legal scholars are trained to think in terms of a "field" or an "area" of law (Rechtsgebiet, branche du droit). Its origins can be traced back in Justinian's *Corpus Iuris Civilis* (529AD); Grotius famously founded international law and also discussed the divisions of law in 1625,[83] and updates of Justinian's code directly influenced the 19th century Pandectist School in Germany. Codification of the law[84] became an ideal during the nineteenth century in continental Europe in the meaning of "*setting forth the law in a rational and systematic way, eliminating the disorganization and archaism of traditional law and establishing the natural rights under the protection of an enlightened sovereign*" or, in other words, "*as a way to modernize and rationalize the law into a systematic and self-sufficient repository of legal principle*".[85] The Enlightenment eventually gave birth to, most famously, the French *Code Civil* (Civil Code) in 1804[86] but also to other civil codes across Europe.[87]

Despite this centuries-old European legal tradition on classification, a concrete list of criteria for new legislation to qualify as a new "field of law" does not seem to exist under Roman Law systems – or at least there is no general consensus on its content.[88] In 1847 Thöl placed emphasis on legal sources, and considered as separate fields of law

[83] In De iure belli ac pacis, Paris, 1625.

[84] The issue of codification of the law (see Weiss, 'The Enchantment of Codification in the Common-Law World'.) is not the same as the issue of legal taxonomy; Although codification work builds upon legal taxonomy findings, whether to have distinct fields of law and whether the law should be codified are essentially two different questions. However, the merits and the criteria of legal codification could be of indirect use also to the discussion on legal taxonomy, and as such they are being used in this analysis.

[85] Craig M Lawson, 'The Family Affinities of Common-Law and Civil-Law Legal Systems', *Hastings International and Comparative Law Review* 6 (1982): 49., p.93 and 119 respectively; See also Weiss, 'The Enchantment of Codification in the Common-Law World'. pp.452-453. On the importance of a system from a Roman law point of view, where "reason" retains its central role, see particularly Karl Larenz and Claus-Wilhelm Canaris, *Methodenlehre Der Rechtswissenschaft* (Springer, 1995).pp.263-264, and also Claus-Wilhelm Canaris, *Systemdenken und Systembegriff in der Jurisprudenz: entwickelt am Beispiel des deutschen Privatrechts*, 2., überarb. Aufl, Schriften zur Rechtstheorie 14 (Berlin: Duncker & Humblot, 1983)., pp.11ff.

[86] The Napoleonic Code; The Civil Code was accompanied by its, perhaps not as famous but equally influential, Code of Commerce (1808), Code of Civil Procedure (1806), Code of Criminal Procedure (1811) and the Penal Code (1811).

[87] See the Austrian Civil Code of 1811 or the Prussian Code of 1974.

[88] In spite of the fact that this has been a repeated legal quest particularly in German legal theory (see, indicatively, Wolfgang Winkler, 'Das Agrarrecht, Sein Gegenstand Und Seine Stellung in Der Rechtsordnung', in *Recht - Umwelt - Gesselschaft: Festschrift Fur Alfred Pikalo*, ed. Gunther Frohberg, Otto Kimminich, and Robert Weimar (Berlin: J. Schweitzer Verlag, 1979), 363-.; Ines Härtel, 'Energieeffizienzrecht – ein neues Rechtsgebiet?', *Natur und Recht* 33, no. 12 (1 December 2011): 825–33, https://doi.org/10.1007/s10357-011-2179-7.HEINHARD STEIGER,

only these whose sources are different and distinguishable from others.[89] One century later, Ruthers identified a new field of law through existence of a system ("materiales Ordnungsssystem").[90] Mellwitz, in an influential dissertation of 1965, introduced four criteria for identification of a new field of law, namely (i) Existence of a new legal object with unique characteristics, that are derived from special aims and purposes, real-life circumstances, legal rights and values; (ii) specialised new notions and guidelines, (iii) a unique method, and (iv) a closed system, before going on and denying such status to Air Law.[91] In a largely similar approach, Hondius, while examining in 1980 whether a new legal field on "data law" has emerged, identified as relevant three criteria, (a) the application of predetermined rules and procedures to varying constellations of facts and conditions, (b) existence of a system, ie. groups of related and interacting subjects, and (c) development of problem-solving techniques.[92] Other authors look for a practical real-life need accompanied by strong theoretical work interconnecting and forming a system out of connected pieces of legislation.[93] Finally, a more practical approach searches for enough experts, laws, case law and legal writing that altogether create a perception, if not conviction, of a "legal field".[94]

Because the notion of a "system" is common to all of the above listings of criteria for designation of a new field of law, it is perhaps important to discuss its meaning within legal context. Larenz and Canaris distinguish between an "outer" and an "inner" system within law.[95] The "outer" system refers to structure and order of the law's subject-matter, in the sense that abstract legal principles and notions are particularised onto a specific context;[96] The legal actors, the scope of the law and its objectives are set horizontally for the whole field, in a so-called "*general part*".[97] Once this has been accomplished, an "inner" system of rules and principles along with a corresponding system of legal concepts that form a specific "way of thinking" and affect doctrinal, judicial, and legislative development of the law come into play.[98] Admittedly, Larenz and Canaris, being Civil Law professors themselves, adopted a bottom-up perspective, meaning

'Umweltrecht — Ein Eigenständiges Rechtsgebiet?', ed. Michael Kloepfer, *Archiv Des Öffentlichen Rechts* 117, no. 1 (1992): 100.; Karl August Bettermann, *Das Wohnungsrecht Als Selbstandiges Rechtsgebiet* (TÜBINGEN, J.C.B.MOHR, 1949).

[89] Thöl J H, Das Handelsrecht, Band 1, 1847, p.14-15.

[90] Reference in Milos Vec, 'Kurze Geschichte Des Technikrechts', in *Handbuch Des Technikrechts*, ed. Martin Schulte, Abteilung Rechtswissenschaft (Berlin Heidelberg: Springer-Verlag, 2003), https://doi.org/10.1007/978-3-662-07707-8. p.5, himself also dealing with the question whether technology law is a separate field of law.

[91] Frauke Mellwitz, 'Voraussetzungen Einer Rechtswissenschaftlichen Disziplin - Angewandt Auf Das Luftrecht', (Thesis, Goettingen, 1965). cited in Winkler, 'Das Agrarrecht, Sein Gegenstand Und Seine Stellung in Der Rechtsordnung'. p.372.

[92] Hondius, 'Data Law in Europe'. P.87.

[93] Roland Norer, 'Agrarrechtliche Sonderrechtstheorie, Funktionale Theorie Und Das Recht Des Ländlichen Raums', in *Reichweite Und Grenzen Des Agrarrechts*, ed. José Martínez (Nomos Verlagsgesellschaft mbH & Co. KG, 2018), 111–32, https://doi.org/10.5771/9783845291819-111.p.115. The same was, for example, the case on the Wohnungsrecht, developed after the lack of residences in Germany in the aftermath of the Second World War (see Bettermann, *Das Wohnungsrecht Als Selbstandiges Rechtsgebiet*.) Or, see also Burgi M, Ein Rechtsgebiet wird erwachsen: Zur Umsetzung der neuen EU-Vergaberichtlinien, Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR), 2014.

[94] See Härtel, 'Energieeffizienzrecht – ein neues Rechtsgebiet?' with further bibliography.

[95] Larenz and Canaris, *Methodenlehre Der Rechtswissenschaft*. pp.263ff..

[96] Larenz and Canaris., p.265.

[97] *Larenz and Canaris.*, p.267.

[98] *Larenz and Canaris.*, pp.317-318.

that their starting point was legal provisions found in the Civil Code and their classification, rather than a top-down, whereby a legal taxonomy is created from scratch. Despite their perspective, however, their distinction between an "outer" and an "inner" system is critical also for designation of a legal field purposes.

2.3. Conclusion: Criteria (and justification) for identification of a new legal field

In view of the above, **the criteria that seem to emerge from a comparative analysis for designation of a new field of law both under Roman and Common Law perspective (under the above clarifications) could basically refer to (i) *Commonality*, (ii) *Systemic distinctiveness*, (iii) *Public perception*, and (iv) *Transcendence*. Existence of these criteria should be established cumulatively; Occurrence of only one or more would not suffice for acknowledgment of a new legal field**.

Commonality, a term used by Aagard, refers to a "*set of characteristics shared in common by the situations that arise within the area of law that the field encompasses*". It relates to Levine's "*society facing a significant body of interrelated problem which could benefit from a unified legal treatment*". It also reflects Hondius' "*application of predetermined rules and procedures to varying constellations of facts and conditions*" and Mellwitz's "*existence of a new legal object with unique characteristics derived from […] real-life circumstances*".[99] Essentially, then, a commonly identified social problem in need of a unified legislative solution.

Systemic distinctiveness shares again from Aagard's approach ("*the field is governed by unique legal rules that apply only within the field (field exceptionalism)"*) and from the requirement for uniqueness of its sources, however it also requires that these unique legal rules be organised in a system in the Roman Law tradition as detailed by Canaris. Therefore, this is practically a double criterion, whereby unique rules and existence of a system needs to be confirmed. Needless to say, the system itself need not be unique; Distinctiveness is granted by the uniqueness of the rules in it; It is simply its existence that needs to be established. Apparently, this is a requirement almost invariably required by all legal scholars that dealt with the issue of identifying what differentiates a legal field from standalone pieces of legislation.

[99] Mellwitz, 'Voraussetzungen Einer Rechtswissenschaftlichen Disziplin - Angewandt Auf Das Luftrecht',.

Public perception pertains to empirical observation. In practical terms it is best explained by Levine ("*what lawyers do, what clients want, existence of separate courts, a group seeing itself as deserving separate legal treatment*"). It broadly reflects the perception of the legal profession: Essentially, if enough lawyers and practitioners identify themselves as exercising a particular field of law and if enough legal scholars consider themselves experts in a particular field of law, then existence of this legal field would, at least, merit examination.

Finally, ***transcendence*** is perhaps a vanity criterion. A literal interpretation of Easterbrook's expectation that "*legal fields should illuminate the entire law*" would set the bar too high for any newcomer. However, raising the bar could be useful in order to meet the "Law of the Horse" threshold.

The above criteria largely address also the issue of the merits of a legal taxonomy. A legal taxonomy is taken for granted in Roman Law systems, where classification is inherent since the time of Imperial Rome and therefore its merits are unquestioned. On the contrary, in Common Law systems the merits of a legal taxonomy would most likely pertain to improving implementation under a systematic approach: A legal field implies a separate, standalone and specific system, complete with its own system-specific principles and rules of general, horizontal application. Acknowledgement therefore of a new legal field would mean that practitioners and stakeholders would be assisted in applying the law, thus leading to legal certainty.

3. Is data privacy law a new field of law? Applying the *data privacy law acquis* onto the legal field criteria

This section aims to apply the criteria identified above (*commonality*, *systemic distinctiveness*, *public perception*, and *transcendence*) onto data privacy law in order to assess whether it merits to be treated as a legal field. In order to do so attention will be given to the *data privacy law acquis*. The *data privacy law acquis* refers to the bare common characteristics of a data privacy law in order for it to be recognized as such.[100] What are the unique characteristics of a data privacy law as formulated over the past fifty years since introduction of the first relevant legal instrument and shared by now anywhere one is met?

There is a number of ways through which to derive these distinctive characteristics: An obvious one would be a comparative analysis of the international instruments at hand, namely the EU, the Council of Europe, the UN, the OECD and the APEC data privacy models. While presumably this is the case behind the UN Index, the UN does not provide any concrete list in this regard.[101] Fortunately, Greenleaf's global index provides certain specific criteria: These are "*(a) the basic data privacy principles (rights to access and correction, the finality principle, the security principle and as many other principles as possible from the combined list of the Council of Europe and OECD models), plus (b) some method of enforcement, incorporated into one or more laws on a country's private sector or public sector or both*".[102]

[100] See also Vagelis Papakonstantinou and Paul De Hert, 'The Regulation of Digital Technologies in the EU: : The Law-Making Phenomena of "Act-Ification", "GDPR Mimesis" and "EU Law Brutality"', *Technology and Regulation* 2022 (2022): 54, https://techreg.org/article/view/11459.

[101] The explanatory text in the respective questionnaire reads as follows: "*Privacy may be defined as the claim of individuals to determine when, how and to what extent information about them is communicated to others. It is the right of an individual to control what happens with their personal information. Privacy laws are also known as, or supplemented by, Data Protection laws. Many laws are influenced by international models, such as the OECD Privacy Guidelines, the Commonwealth model law on privacy, the EU Data Protection Directive, the African Union Convention on Cyber Security and Personal Data Protection, ECOWAS Supplementary Act on personal data protection (A/SA.1/01/10), Council of Europe Convention 108 and APEC Privacy Framework*"; Each country therefore has to self-assess whether it falls under the above description (information from https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide, accessed on Winter 2021).

[102] Greenleaf, 'Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority'.; An understanding of "*common features*" for new data privacy laws was evident in the relevant academic community since their first release (see, for example, Bing, 'Information Law?' p.232;

These criteria, in fear of coinciding in full with personal data protection notions,[103] ought to be complemented by yet another characteristic, namely explicit acknowledgement in the texts of the laws under examination that respect for private life falls within their scope. Therefore the *data privacy law acquis* would have to be re-formulated as including (a) laws that self-identify themselves as protecting (or at least observing) private life, (b) the basic data privacy principles, and (c) a method of enforcement.

A point that needs to be noted refers to the fact that, unavoidably, the above *acquis* includes also the European data privacy nomenclature (e.g. "*controller*", "*processor*", "*data subject*")[104] as well as a certain legal methodology (e.g. identification of a legal base for the processing), if at least they are to become at all operable. For example, the right to access would have little meaning if the notions of "*data subject*" and "*data controller*" were not recognised as well; Or, the principle of lawfulness would not mean much if the notion of "*consent*" was not acknowledged. In other words, the list of characteristics comprising the *data privacy law acquis* is necessarily accompanied by a European legal toolset without the assistance of which they could not develop their, expected, effect (and which is, in itself, assessable under the *systemic distinctiveness* criterion analysis below).

Once it has been established whether data privacy law is a new legal field attention will be given, first, on the (formalistic) question of its content and placement, and then, on the practical merits of such finding.

See also Anneliese Roos, 'Core Principles of Data Protection Law"', *Comp. & Int'l L.J. S. Afr.* 39 (2006): 102–30. for application of this *acquis* in third countries, namely South Africa.

[103] See the analysis in subsection 3.5 that follows, where personal data protection law is considered a subfield of data privacy law.

[104] See, for example, Michael Birnhack, 'Reverse Engineering Informational Privacy Law', *Yale Journal of Law & Technology* 15, no. 24 (2012)., who considers the definitions and the actors of the DPD its "*building blocks and legal structure*" (p.42).

3.1. Commonality

Essentially, the criterion of commonality refers to a commonly identified social problem in need of a unified legislative solution. As such, it appears to be easily fulfilled by data privacy law: The erosion of privacy in the digital realm is a globally identified problem; Data privacy law is the globally accepted regulatory response to it.

Data privacy law emerged as a response to automated personal data processing and the digitisation of personal information.[105] While concerns about the protection of privacy by technological advances (in fact, photography) were expressed as early as in 1890,[106] it was digital technologies and the exponential increase in humanity's processing capacity that caused the first personal data protection acts to emerge in Europe. Consequently, while the social problem of the protection of privacy against unwarranted processing of personal information was well identified outside the confines of data privacy, it was specifically automated data processing and the digital realm that decidedly turned the legislators' interest on privacy, leading to the first data privacy laws.

The social problem behind the release of data privacy laws has not changed in the meantime:[107] Today the protection of their personal data and privacy is customarily found high on the lists of concerns affecting individuals both at national and at international level. A basic characteristic of these concerns is their shared understanding of the problem at hand: Information technology applications and contemporary business models involving personal data processing have become globalized; Internet social networks directly affect the lives of billions; Processing in one country or on the cloud affects directly all others. Therefore, the social problem lying at the heart of data privacy is shared in its totality both in Europe and across the globe.

[105] See footnote nr.32.
[106] The famous Warren and Brandeis article on the right to privacy was written because of unauthorised photography of the wedding of Brandeis' daughter, leading the authors to note that "*numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops*" (p.195)
[107] See Bennett, *The Privacy Advocates*., pp.9-21.

3.2. Systemic distinctiveness

Systemic distinctiveness is practically a double criterion for identification of a new field of law: It requires both unique legal rules ("*field exceptionalism*", in the words of Aagard)[108] as well as existence of a legal system, along the lines described by Larenz and Canaris. Data privacy law qualifies both: The *data privacy law acquis* includes a unique set of legal rules, that make it immediately identifiable and distinguish it from any other field of law. As regards the second requirement, data privacy law profits from both an "*outer*" and an "*inner*" legal system that have practically accompanied it since it first emerged.

Field exceptionalism within data privacy law is warranted through, essentially, the *data privacy law acquis* itself: its basic principles (fair and lawful processing, purpose specification principle, data minimization principle etc.) are unique to the data privacy field – they are not to be found in any other field of law even if it is involved in information technology-related regulation.[109] Similarly, the legal toolset necessary for these to function (essentially, the data privacy nomenclature) is also unique to the data privacy field. Even terms that can be met in other fields of law as well, such as "*consent*", have a unique meaning within the data privacy law context.

As regards existence of a system, evidence of both an "*outer*" and an "*inner*" system may be found within data privacy law. As regards an "*outer*" system, in the meaning given to it by Larenz and Canaris[110], abstract legal principles and notions such as proportionality, accountability, transparency or self-determination are particularized within the data privacy context into specific legislative provisions, constituting in fact its premises.[111] As regards the data privacy "*inner*" system, this essentially takes form in the legal methodology imposed by the *data privacy law acquis*:

[108] Aagaard, 'Environmental Law as a Legal Field: An Inquiry in Legal Taxonomy'., p.244.
[109] For example, the principle of security is different in data privacy law than in cybersecurity legislation 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', *Computer Law & Security Review* 35, no. 6 (2019).
[110] See footnote nr. 95.
[111] For example, with regard to self-determination, the basic German census case and its effect on the, then nascent, data privacy, see, indicatively, Jan Philipp Albrecht, 'Uniform Protection by the EU – The EU Data Protection Regulation Salvages Informational Self-Determination', in *Data Protection Anno 2014: How to Restore Trust?*, ed. Hielke Hijmans and Herke Kranenborg (Intersentia, 2014), 117.

Specifically, practitioners while applying data privacy law are basically called to think in terms of, first, establishing a lawful legal basis for personal data processing (consent or law) and then applying the data privacy principles onto a specific processing operation while at all times protecting a fundamental human right, that of private life (accompanied by the right to data protection, if within the EU). This legal methodology reflects the internal organisation of data privacy law and is visible in all of its implementations across the globe. In essence, it formulates a unique, systematic way of thinking that affects all practitioners and stakeholders within the field.

3.3. Public perception

The *public perception* criterion essentially reflects the practices and expectations of the legal (or other, as the case may be) professionals that are active in the field. In essence, it requires that enough lawyers and practitioners identify themselves as exercising a particular field of law, and also that enough legal scholars consider themselves experts within the same. Notwithstanding naming unclarity, as detailed in Section 1 of this analysis, the fact is that the introduction of the GDPR has created a significant compliance market, or a "privacy industry",[112] composed of lawyers, technologies, as well as, an entirely new profession, that of Data Protection Officers.[113] As regards legal scholars, based only on English-language metrics, a number of international legal journals can be identified carrying the name "privacy" on their title, while dozens of others list explicitly data protection or privacy (in any one of their formulations) among their topics of interest; While a metric for the number of academic books and articles published over the past fifty years is not readily available, in view of the above, institutional, circumstances, it is not expected to be insubstantial.

[112] See, for example, Hughes T, Reflecting on the Growth of the Privacy Industry, IAPP Privacy Perspectives, 12 August 2020.
[113] Admittedly, DPOs were active in Germany since the first Federal data protection act back in 1978, and they were also acknowledged in the DPD text after German insistence (see Simitis, 'From the Market To the Polis: The EU Directive on the Protection of Personal Data'. p.450).

3.4. Transcendence

The criterion of *transcendence* requires that any new field of law, if it wishes to be identified as such, brings a substantial offering, both quantitatively and qualitatively, to the entire law. Although raising perhaps the bar too high, this is a necessary criterion in order to distinguish among fields of law created by necessity or historical circumstances that are aimed at dealing with a specific problem without any lasting effect to the entire law, doomed to disappear or retreat when the relevant problem vanishes.

Data privacy law fulfils this criterion as well. In addition to its long history of implementation, it has produced a fundamental right, the right to personal data protection, to be found both in the Treaty of the Functioning of the EU and in the constitutions of several EU Member States. Even outside Public Law boundaries it is important to note that introduction of the *data privacy law acquis* within any specific jurisdiction is not an isolated, restricted within its specific subject-matter legal event. On the contrary, data privacy law once incorporated into national law produces immediately far-reaching effects, in the sense that several other fields of law are affected by it. Indicatively, telecommunications law, civil law, civil and criminal procedure law are all fields where, in view of the fact that personal data processing takes place for their own aims and purposes, adherence to the rules and principles of data privacy law, once into effect, should be observed also by them. Notwithstanding the fact that the processing of personal data within a specific jurisdiction prior to introduction of data privacy law may have taken place in an unregulated manner or under general rules, once data privacy law is enacted, re-examination of its entire law under the new light is to be expected.

3.5. Data privacy law as a legal field: Content and placement

Once its qualification as a new field of law has been established, as far as its content is concerned, **data privacy law comprises both digital privacy and personal data protection provisions**. As seen above, the notion of privacy within a digital context is broader than the notion of personal data. For example, confidentiality of communications would constitute another, distinct topic within data privacy law.[114] Consequently, data privacy law is a broader legal field that includes personal data protection law.[115] Or, in other words, **personal data protection law should be considered a subfield of data privacy law,**[116] in spite of the fact that, particularly in the EU, it is by far its most developed subfield in terms of volume and sophistication and could perhaps claim legal field status itself. The merits of this classification, of subordinating personal data protection law to data privacy law, apart from lifting doubts over globally-used nomenclature that lasted for decades, will also be felt in EU law, as it will be demonstrated in the subsection that follows.

Once its legal field status has been confirmed and its content has been clarified, data privacy law next needs to be placed within the broader legal system where it belongs. While, again, this might appear an unnecessary exercise in Common Law jurisdictions, under Roman Law classification within a broader legal system carries concrete consequences, most notably because the principles of that broader field also apply onto all legal fields that fall under it. For example, if a field of law is recognized as falling under Constitutional Law then all human rights' theory and principles apply to it as well, in addition to its specific provisions and principles. Exactly that would appear to be the case for data privacy law: **Because its *acquis* pertains to at least one (private life) and in certain cases two (in the EU also to personal data protection) fundamental human rights, it would fall under the Constitutional Law field**[117] (which, in turn, falls under the Public Law field). Consequently, within Roman Law jurisdictions at least, the legal interpretational toolset of Constitutional Law may find application to data privacy law provisions, under a *lex specialis / lex generalis* relationship. This finding carries concrete benefits for data privacy law, as it will be demonstrated in the

[114] See Bing, 'Information Law?' pp.233-235.
[115] In the UN's, correct, wording: "*Privacy laws are also known as, or supplemented by, Data Protection laws"* (see above, footnote nr. 101)
[116] As, straightforwardly, stated in Britannica, on the "*data protection*" entry, "*data protection, species of privacy law that controls access to information relating to the individual*", accessed in Winter 2021.
[117] This was, however, not always the case (see, for example, Bing, who in 1981 noted that "*the European legislation [on personal data protection] is more closely related to the law of public administration than to the law of individual liberties*" (Bing, 'Information Law?' p.232). Similarly, many legal publishers today still classify data privacy law under Administrative Law.

subsection that follows. On the other hand, data privacy law constitutes international law only for these countries that have ratified Convention 108+; In practice, it is only these countries that, in an event of a legal gap or a need of interpretational assistance, may find recourse to the guidance provided by the Council of Europe data privacy legal system.

3.6. The benefits of acknowledgement of legal field status for data privacy law

Having established that data privacy law fulfils all of the above criteria and therefore may be treated as a legal field, and also having elaborated upon its content and placement within a (Roman) legal system, the question remains: What is practically gained from this theoretical exercise? Is this merely a legal theory exercise without any practical implications? Confirmation of legal field status is merely a vanity concern of its practitioners? Or does it present concrete results for everyday practice? This subsection will attempt to address this question: specifically, **benefits to acknowledgement of legal field status for data privacy law come in addressing concrete problems of *form*, *interpretation* and *implementation***.

Gains in *form* are perhaps the easiest to establish. In essence, they remove the requirement for self-sufficiency of standalone data privacy laws, which leads to some awkward law-making. A comparative review of all EU data privacy legal instruments reveals a typical structure: A first part (or chapter) on the data privacy definitions is followed by a second part on its basic principles; Next follow parts on cross-border data transfers, national implementation and international cooperation respectively.[118] The problem in this case is that, if data privacy law is introduced in more than one legal instruments (for example, separating between general and security-related processing, or separating between Member State and EU law), reference needs to be made to the above basic provisions by means of a tedious copy-paste exercise each time: For example, the provisions on the personal data protection definitions or the lawfulness of processing[119] are copied-pasted within all three basic EU texts.[120] However, under a legal field status approach it would be possible to distinguish between "general" and "specific" data privacy law. "General data privacy law" could then be included in a single legal instrument that would apply horizontally all over the field, enabling all other "specific" data privacy legislation simply to refer to it instead of repeating its provisions. In this way not only form but also substance of the law would become more efficiently organised: In an event of an amendment in the "general" data privacy law, rather than having to update all "specific" data privacy laws individually, indirect reference

[118] See Chapters I – V of the GDPR; Chapters I – V of the LED; Chapters I – IV of Convention 108+; Parts One – Four of the OECD Guidelines.
[119] See Articles 4 of the GDPR and 5 of Regulation 1724/2018 respectively, as well as, for most of its part, Article 4 of the LED.
[120] See, for example, the article on definitions in the GDPR (Article 4) the LED (Article 3) and Regulation 1725/2018 (Article 3), where all common items are copied-pasted. Large chunks of copied-pasted text can be viewed in the above three instruments in other cases, as well, e.g. on their provisions on supervisory authorities or data transfers.

to it in their respective texts would warrant that, whenever its provisions change from time to time, other data privacy provisions would be automatically updated as well.

Particularly within EU law, distinction between "general" and "specific" data privacy within the context of a data privacy law field would address the legislators' need to include technical, detailed provisions in general data protection texts. This is most demonstrably the case in the establishment and organisation of supervisory authorities (Data Protection Authorities, "DPAs"). A substantial part of any EU and Member State personal data protection act is dedicated to not only establishment but also operational details of its DPA(s),[121] going into such detail as duty of professional secrecy[122] or duration of the term of its members.[123] Notwithstanding the importance of these topics, their place is not next to the most basic data protection principles and rules but rather in a secondary, specialized piece of legislation. However, today they occupy a necessary and unavoidable part of personal data protection laws, because, in lack of legal field acknowledgement, each one of them needs to be self-sufficient. In the event of legal field acknowledgement, a "general" law would include the basics while all issues of secondary importance, such as DPA day-to-day operation, could be dealt with in secondary pieces of legislation.

Interpretational gains come in the form of systematic interpretation that would become acceptable. In other words, a field of law comes complete with horizontally applicable principles and provisions whereas a standalone piece of legislation (even as comprehensive as the GDPR) needs to be interpreted exclusively on its own merits. Therefore, in the event of a GDPR provision that may be lacking in its wording interpretational assistance could come by recourse to general principles and rules within the broader data privacy or even Constitutional Law field. Legal field status therefore offers an important interpretational tool in this regard. Finally, *implementation* gains in formal acknowledgement of legal field status for data privacy law pertain to legal gaps' elimination, predictability and legal certainty. While in their totality an elusive ideal, is greatly assisted by systematic thought and application of general principles to complement case-specific provisions so as to reduce to the barest minimum the cases where the law has nothing to say.[124]

[121] See Chapter VI of the GDPR, Chapter VI of Regulation 1724/2018 and Chapter VI of the LED.
[122] See Article 54.2 of the GDPR
[123] See Article 54.1(d) of the GDPR.
[124] See also Larenz and Canaris, *Methodenlehre Der Rechtswissenschaft*. p.275

Conclusion

Data privacy laws were first introduced in the early 1970s as standalone but ambitious pieces of legislation. Legislators could not have foreseen the internet or today's data deluge,[125] but did sense that something of great potential was emerging. In the fifty years that lapsed personal data protection developed into a fundamental human right in the EU legal system, different to that of privacy, while the limited standalone texts of the past became powerful legal documents, most notably the GDPR and the LED, aiming at regulating any and all processing of personal data. The Council of Europe has in the meantime developed the only internationally binding data privacy legal instrument, Convention 108+, that is open to ratification to European and non-European states alike.

In spite however of these important achievements, data privacy laws over the past fifty years have not addressed such basic problems as defining their exact content or even reaching a commonly accepted name. **The initially preferred term in Europe, "data protection", is no longer suitable because today "data" protected by law may include non-personal data as well, therefore this term at the very least would have to be replaced with "personal data protection" (making, for example, the GDPR the GPDPR). However, even this terminological fix would not be enough: The bond with privacy seems unbreakable**. Even within EU nomenclature privacy and personal data protection seem inseparably connected in the minds and hearts of legislators and the public alike. The CoE has no problem acknowledging this relationship in its influential Convention 108+. Outside Europe there is clear and strong preference for the word "privacy" or any other of its derivatives (information(al) privacy, data privacy) to include personal data protection as well. **Taking these into account it is hereby suggested that the new field of law should be named "data privacy law", a term that meets expectations while also avoiding interpretational pitfalls that the terms "privacy" or "information(al) privacy" would entail**.

[125] See *The Data Deluge*, The Economist, 27 February 2010.

The above leave the question of a new legal field open. Admittedly, however, this question is far more pressing in Roman than in Common Law systems. The merits of a legal taxonomy are highly debated within Common Law systems, where the law is perceived as a seamless web. On the contrary, Roman law systems are organised systematically into fields of law under an unbroken logic that dates back to Imperial Rome. Notwithstanding their fundamentally different approaches, however, if Common Law systems were willing to discuss the case of a legal taxonomy then a list of common criteria for a legal field to be recognized as such could be derived between the two: **These would pertain to *commonality*, *systemic distinctiveness*, *public perception* and *transcendence***.

Data privacy law qualifies all these criteria. The relevant analysis reaches this conclusion taking into account the worldwide *data privacy law acquis*. In essence, data privacy law is characterized by *commonality* on the social problem it addresses and the legal solutions applicable to it, in the sense that the erosion of privacy in the digital realm is a globally identified problem and data privacy law is the globally accepted regulatory response to it. It is also characterized by *systemic distinctiveness* both in terms of exceptionalism of its provisions and in terms of existence of an "outer" and "inner" system within the legal methodology applicable to it. *Public perception* is indeed one of a separate field of law in both practice and study. Finally, as regards the *transcendence* criterion, data privacy law has developed a horizontal effect to the entire law in each jurisdiction it is met.

Once legal status field has been established the questions that next need to be answered refer to its actual content as well as to its proper placement within a system of (Roman) law. As far as its content is concerned, data privacy law comprises both digital privacy and personal data protection provisions, the notion of privacy in a digital context being broader than the notion of personal data. Consequently, data privacy law is a broader legal field that includes personal data protection law – or, in other words, personal data protection law should be considered a subfield of data privacy law, even within the EU where personal data protection has fought for, and won, its autonomy. Finally, because its *acquis* pertains to two fundamental human rights (protection of private life and data protection), data privacy law would fall under the Constitutional law field.

None of the above classifications would matter if they were not accompanied by concrete benefits for the law concerned. Benefits to acknowledgement of legal field status for data privacy law come in addressing concrete problems of *form*, *interpretation* and *implementation*. Gains in *form* can be identified through a comparative review of most data privacy legal instruments in effect today: Repetitions through extensive copying-pasting of basic provisions among data privacy laws, as well as technical, administrative sections embedded in basic data privacy

provisions would be avoided if legal status was acknowledged whereby a "general" and "specific" data privacy law would enable automatic cross-referencing. *Interpretational* gains come in the form of systematic interpretation while *implementation* gains refer to legal gaps' elimination, predictability and legal certainty. For as long as our technological environment remains in constant flux, such adaptability, that is far better achieved within a legal field than in standalone solitary legislation, is perhaps the most important gain of all.