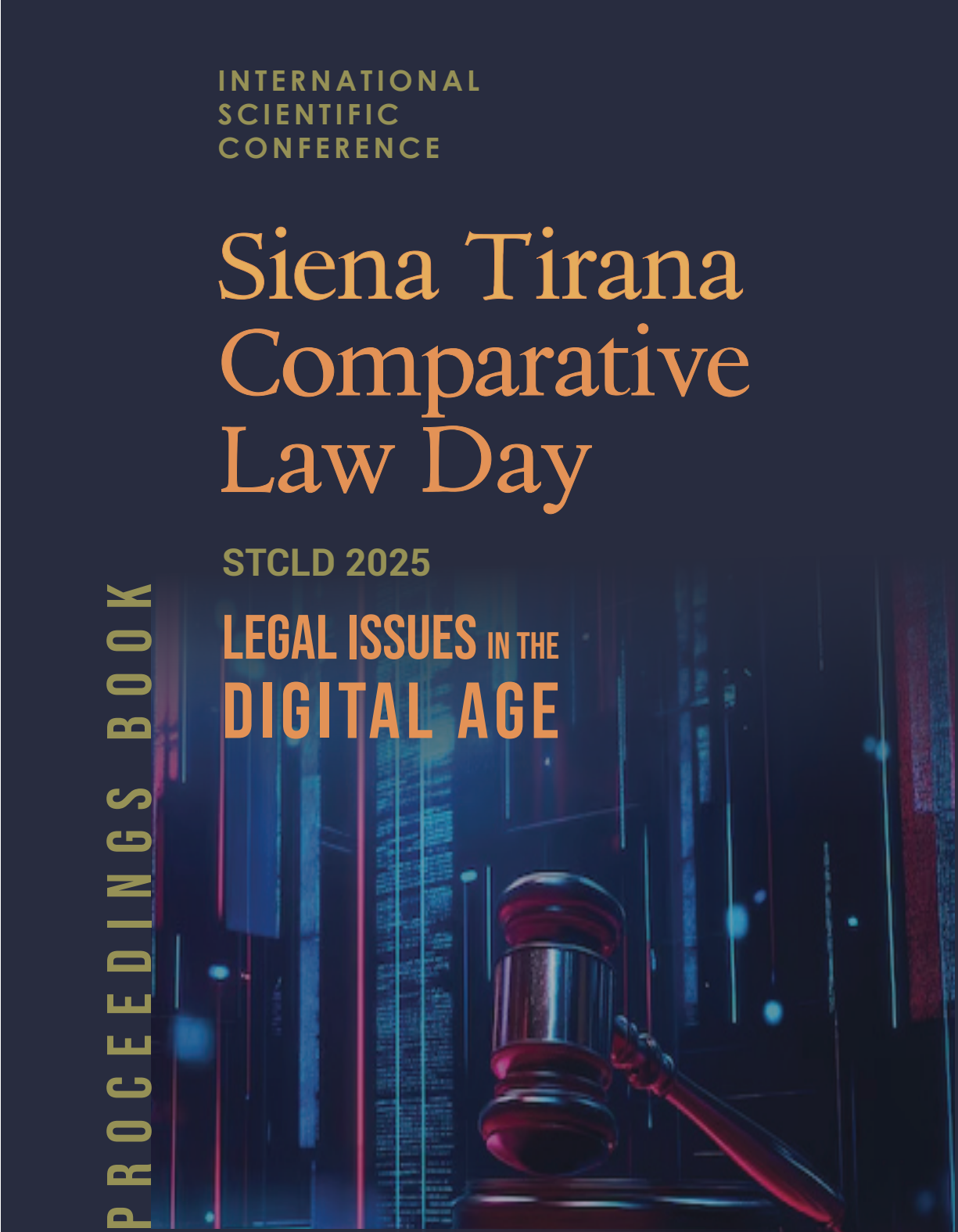
INTERNATIONAL
SCIENTIFIC
CONFERENCE

Siena Tirana Comparative Law Day

STCLD 2025

LEGAL ISSUES IN THE DIGITAL AGE

PROCEEDINGS BOOK



UNIVERSITÀ
DI SIENA
1240

UNIVERSITÀ DI SIENA
1240

DIPARTIMENTO DI GIURISPRUDENZA — DGIUR

UNIVERSITY OF SIENA,
DEPARTMENT OF LAW

UNIVERSITY OF TIRANA, FACULTY OF LAW,
DEPARTMENT OF CIVIL LAW

International Scientific Conference

"Siena-Tirana Comparative Law Day"

Legal Issues in the Digital Age

STCLD 2025

16 May 2025
Siena - Italy

PROCEEDINGS BOOK

Tirana, 2025

UNIVERSITÀ DI SIENA 1240 — DIPARTIMENTO DI GIURISPRUDENZA — DGIUR

UNIVERSITY OF SIENA,
DEPARTMENT OF LAW

UNIVERSITY OF TIRANA, FACULTY OF LAW,
DEPARTMENT OF CIVIL LAW

International Scientific Conference

"Siena-Tirana Comparative Law Day"

Legal Issues in the Digital Age

STCLD 2025

16 May 2025
Siena - Italy

SCIENTIFIC COMMITTEE

Prof. Dr. Artan Hoxha, University of Tirana, Albania
Prof. Dr. Dorina Hoxha, University of Tirana, Albania
Prof. Alessandro Palmieri, University of Siena, Italy
Prof. Dr. Kestrin Katro, University of Tirana, Albania
Prof. Assoc. Renata Tokrri, University of Tirana, Albania
Prof. Valeria Piergigli, University of Siena, Italy
Prof. Giammaria Milani, University of Siena, Italy
Prof. Paolo Guarda, University of Trento, Italy
Prof. Dr. Eriona Katro, University of Tirana, Albania
Prof. Assoc. Anjeza Liçenji, University of Tirana, Albania
Prof. Assoc. Ersida Teliti, University of Tirana, Albania
Prof. Assoc. Artan Saphiu, University of Tirana, Albania
Prof. Assoc. Ilda Melo, University of Tirana, Albania

PROCEEDINGS BOOK

ISBN 9789928826800

Tirana, 2025

Content

Collective privacy litigation and the law of torts. A comparative perspective

Alessandro Palmieri
Marina Federico[1*]

Abstract

The present paper is aimed at highlighting the pivotal role of aggregate litigation in the field of personality rights. Especially in the current age, characterized by large online platform operators, with significant market share and influence, infringements of data protection rules in the telematic highways are likely to be harmful to a substantial number of data subjects. Therefore, class actions, where available, and other collective means of grouping individual claims, are the only credible way to stop illegal behaviour. After having outlined the general framework, comparing the EU and the US legal systems, and having analysed the interactions between data protection and tort law, the Authors focus on an emblematic judicial dispute, whose observations shoes the vitality of collective redress mechanisms.

Keywords: *Data protection, Privacy, Tort law, Aggregate litigation, Class action*

1. The collective dimension of data protection in the age of Big Techs

At the beginning of the current century, a scholar based in the United States observed that: 'The threat to personal privacy caused by the ever-expanding flow of personal data online is the most significant public policy concern spawned by the Internet'[2]. After more than two decades – that have witnessed the rise

[1] * Whilst the paper reflects the shared views of the Authors, paragraphs 1 and 5 are to be attributed to Alessandro Palmieri; paragraphs 2, 3, and 4 to Marina Federico.

[2] S Hetcher 'Changing the Social Meaning of Privacy in Cyberspace' (2001) 15 *Harv. J.L. & Tech.* 149.

of platforms (and platform capitalism)[3], as well as the triumph of the so-called BigTechs, which have acquired hegemony in various (almost all) digital market segments, including those related to the Artificial Intelligence supply chain[4] – the aforementioned statement is still correct. Actually, some critical issues, instead of being solved, have become more serious. In a constantly evolving scenario, what seems now clear is the fact that information plays a crucial role. The media, and some commentators, have identified data with the 'new oil'. Although one can observe several fundamental differences between the two types of commodities, the metaphor is suggestive. This can be said especially of 'big data'.[5] And in the vast area of 'big data' we find pieces of information that fall into the realm of personal data.

Hence, the economic value of personal data is rather unanimously acknowledged in the relevant literature. This value is susceptible to be further increased in step with the expected development of the technological paradigm of Internet of Things (IoT)[6]. Indeed, the academic debate over personal data as counter-performance is rich and growing.[7] Apart from the consideration that the average data subject, involved in her/his usual online activities does not perceive such value, and is even less able to quantify it, when we turn to the assessment of damages arising from an infringement of data protection rules, another troublesome factor needs to be taken into account.

Examining the situation from the viewpoint of a single person, in many cases the pecuniary losses are minimal; the same goes for non-pecuniary losses, that is to say losses which are not readily measurable in terms of money. The market

[3] See, for instance, A Carstens, 'Regulating big tech in the public interest' (2022) 274 *SUERF Policy Brief*: 'One of the most striking features of the digital economy is the rise of large digital platform companies.

[4] Recently, L Gambacorta and V Shreeti 'The AI supply chain' (2025) 154 *BIS Working Paper*, have underlined that: 'Perhaps the most notable development in the AI market is the increasing influence of (especially US and Chinese) big tech companies across the AI supply chain. Big tech already hold market power in many digital markets and are extending it to emerging AI markets' (p. 9). According to the Authors, the said accumulation of power in the AI supply chain (which consists of five key layers: hardware, cloud infrastructure, training data, foundation models and AI applications) 'poses several risks, including reduced consumer choice, control of the direction of innovation by a handful of firms, operational vulnerabilities, increased cyber security threats and potential financial instability' (p. 13).

[5] See A Marciano, A Nicita and G.B. Ramello, 'Big data and big techs: understanding the value of information in platform capitalism' (2020) 50 *Eur J Law Econ* 345.

[6] See A Becerril 'The value of our personal data in the Big Data and the Internet of all Things Era' (2018) 7(2) *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal* 71.

[7] Among the others, see Á Bueno Biot, 'La contraprestación en forma de datos personales: el nuevo paradigma en la era digital' (2025) 22 *Actualidad Jurídica Iberoamericana* 1122; SM Lener 'Personal data as counter-performance in exchange for contents or services after amendments to the Italian Consumer Code' (2024) *Rivista di diritto privato* 135; J Renko 'Personal Data as Means of Payment for Digital Content or Digital Services in the Slovenian Implementation of the Digital Content and Services Directive' (2024) 74(5-6) *Zbornik Pravnog fakulteta u Zagrebu* 921.

price for raw, and disaggregated, data is low,[8] tending to zero (although very rarely equal to zero), in the overwhelming majority of contexts.[9] And, although it is undeniable that data subjects are able to seek compensation for distress, even in the absence of an economic loss, in all the legal systems where punitive damages are not acknowledged, the sum of money awarded is likely to be modest.

This is not a good reason to deny any kind of redress, as clarified by the Court of Justice with respect to the EU legal systems. Of course, the smallness of the injuries undermines dramatically the incentives to sue potential tortfeasors, which might think to enjoy a *de facto* immunity from civil liability and behave accordingly.[10] By means of illustration, in an action brought by a German data subject, who asked to be compensated for the loss incurred as a victim of the 'Facebook data leak' that in 2021 exposed information (e.g., phone numbers, locations, birthdates) of more than 533 million users of the social network, the German Supreme Court (*Bundesgerichtshof*), while not defining the case, recently found that a sum of 100 euros was suitable for the injured party, whose complaint were focused on the loss of control over the data.[11] On the one hand the judgment at stake can be seen as a victory on a point law for data subjects; but, on the other hand, since the outcome is far away from a high figure, the prospects for an ordinary plaintiff are not so encouraging. Moving on to English law, in an important case concerning the disclosure of data about the involvement of an individual in an ongoing fraud investigation, the claimant was awarded £ 250 (about 290 euros).[12]

The other side of the coin is represented by the fact that, when we come to consider the fraction of infringements ascribable to BigTechs, their customer base is extremely large, and it is composed to a great extent of natural persons. Therefore, a sizeable number of violations of data protection rules is capable of hurting a considerable number of people, and the overall loss becomes significant.[13] In other

[8] D Zetzsche, R Buckley and D. Arner, 'The rise of TechFins: regulatory challenges' in J Madir (ed), *FinTech. Law and Regulation*, 3rd ed. (Edward Elgar 2024), 415, 'the market price for raw data creates little economic incentive for customers to support data sovereignty'.

[9] Taking into account data mining, it has been observed that 'raw data is often compared to crude oil-abundant in quantity, yet unwieldy and of little value until refined. Just as oil undergoes various processes to be transformed into useful fuel, data too requires a series of steps to be made usable for mining': cfr. *Mastering Data Mining* (Cybellium, 2023) 19.

[10] See, for instance, SB Burbank, S Farhang and HM Kritzer, 'Private Enforcement' (2013) 17 *Lewis & Clark Law Review* 637, 674: 'In the scenario in which statutory violations produce a large number of small injuries, compensation may not be a plausible goal, but the absence of representative litigation can render the violator, as a practical matter, immune from suit by private parties'.

[11] BGH - VI ZR 10/24. On this judgment, delivered on 18 November 2024, see G Navone, 'L'illecita pubblicazione di un numero di telefono su Internet è, di per sé, un danno immateriale?' (2025) *Foro it*. IV, 102.

[12] *Driver v Crown Prosecution Service* [2022] EWHC 2500 (KB).

[13] See. A Ruda-González, 'Liability for the unauthorised use of personal data in social networks: the case for collective redress' (2020) *European Journal of Privacy Law & Technologies - Special Issue* 80, 83: 'When considered in an isolated way, harm is very small indeed. Therefore, from an economic perspective each individual affected has little incentives to litigate. However, when considered from a collective or macro perspective, harm is considerable'.

terms, the said violations can be characterized as mass torts. Moreover these firms possess the necessary computational power to process personal information in a way that enables them to extract proper value from such data.

All these factors recommend putting at the centre of attention collective redress mechanisms. Indeed, in Germany, in the aftermath of the said judgment, a consumers' association launched a collective action against Meta Platforms before the Higher Regional Court of Hamburg, in the interest of approximately 6 million users.[14] This strategy has already proved to be successful in Brazil. With respect to an analogous factual background, the State Court of Maranhão (*Tribunal de Justiça do Estado do Maranhão*), at the conclusion a collective civil action, ordered the defendant company to pay 500 reais (about 80 euros) in damages to 8 million users.[15]

2. Information privacy rights and aggregate litigation in Europe and the United States

In the face of the invasiveness and intrusiveness of Information and Communication Technologies (ICTs), individual and consumer rights and freedoms – above all, data protection – are at risk.[16] In this context, collective judicial proceedings are particularly suitable for preventing mass harm, and to redress their possible violations. Among other reasons, this is due to the massive character of the processing of personal data, the high technical complexity of privacy disputes, as well as their costs.

Class actions can grasp the collective dimension of the right to data privacy, beyond the mere idea of 'control' over one's data. They can pave the way towards conceiving data protection as a collective interest of user and consumer groups, as well as a general interest of society in a fair and thriving digital public sphere. Collective proceedings can also tackle 'dispersed' harms, which may otherwise be hard to detect. While harm in consumer cases, if considered individually, might often not seem worth compensating or starting a claim for, its aggregation can

[14] For further information, see the webpage https://www.sammelklagen.de/verfahren/facebook (in German).

[15] Decision of 23 March 2023, nº: 0812915-60.2021.8.10.0001.

[16] On the widespread of ICTs and the consequent changes and adaptations of legal categories to it, see R Bocchini, 'Nuovi beni digitali e mondi dematerializzati. Il metaverso; New digital goods and dematerialised worlds. The metaverse' (2023) 1 *European Journal of Privacy Law and Technologies* 45-54.

give it significance, making it worthwhile to assess whether compensation would be justified.[17]

When looking at collective litigation in this field, from the Brazilian to the European coasts, the reference to the American class action is inescapable. After all, class actions have developed and grown in the United States, where their main features are set out in Rule 23 of the Federal Rules of Civil Procedure. 'Collective privacy litigation' is the term that we believe can effectively encompass the use and role of aggregate proceedings for enforcing data privacy. In American courts, class actions are extensively tested and regularly employed for this purpose. The US has a judicial apparatus that is particularly 'responsive' to changes and needs in society, one in which lawyers and judges actively contribute to the regulation and the handling of political matters. Collective actions have been pivotal in this respect.[18]

Compared to Europe, the US adopts a more 'market-oriented' approach to the regulation of the 'Algorithmic Society',[19] generally leaving more freedom to economic initiative. Meanwhile, the European Union uses extensive regulation for dealing with new technologies to promote a 'rights-oriented' approach.[20] Originally through Directives, later through Regulations,[21] the EU has adopted relevant legal acts in the digital field, with a truly global reach – notoriously

[17] On collective redress in the digital age, see A Palmieri and F Altamura (eds), *Class actions e meccanismi di tutela collettiva. Le prospettive di sviluppo e le sfide della dimensione digitale* (Giappichelli 2023); G Resta, 'Pubblico, privato, collettivo nel sistema europeo di governo dei dati' in G Resta and V Zeno-Zencovich (eds), *Governance of/through Big Data*, vol II (RomaTre-Press, 2023) 606 ff.; M Federico, *Protezione dei dati personali e tutela collettiva. Itinerari di comparazione tra Europa e Stati Uniti* (Giappichelli 2024).

[18] R Kagan, *Adversarial Legalism: The American Way of Law* (Harvard University Press 2001) 16.

[19] This is the expression used by Jack Balkin, in JM Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) *UC Davis Law Review* 1149 ff. On the some of the legal issues arising in the data-driven society, AC Nazzaro, 'L'utilizzo dei Big data e i problemi di tutela della persona' (2018) 4 *Rassegna di Diritto Civile* 1239–1260.

[20] See A Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023); G Finocchiaro, *Intelligenza artificiale. Quali regole?* (il Mulino 2024); R Carleo, 'Piattaforme digitali e contratto – Digital Platforms and Contracts' (2022) 1 *European Journal of Privacy Law and Technology* 76.

[21] The new 'Digital Acts' are, indeed, mostly Regulations. For instance, this is the case of the Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L152/1), the Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data [2023] OJ L2023/2854), the Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act) [2024] OJ L1689/1), the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC [2022] OJ L277/1), the Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/1), to name just a few.

referred to as 'the Brussels effect'.[22] Part of this divergence can also be attributed to the differences between the two systems, as US common law favors regulation through case law rather than written law, which is more typical of European civil law systems.

The protection of personal data and privacy is ensured via Regulation EU/2016/679 (GDPR). One of the distinctive features of the GDPR is its general scope of application. The GDPR regulates and governs the processing of user data, irrespective of the context or the subjects involved. The main rationale of this Regulation is two-fold: to ensure that Europe develops a competitive data-driven economy, while respecting data protection and privacy, acknowledged as fundamental rights.[23]

The US legal framework is radically different. The right to *dignitary privacy*, conceived as the 'right to be let alone', is connected to the protection of personality and non-patrimonial interests. Its protection is assigned to tort law (specifically, to the four torts of invasion of privacy, laid down in the Restatement 2nd of Torts, §652 ff.[24]). Conversely, the protection of personal data, namely *data privacy* or *information privacy*,[25] is framed through a property-like scheme, aligning with the increasing commodification of personal data.[26]

There is no comprehensive statute on data protection or privacy. Besides the privacy torts, US privacy law resembles a patchwork of different rules, both at the federal and state level. The two sometimes overlap in their scope, notwithstanding the application of the doctrine of pre-emption.[27] State laws are sometimes more

[22] A Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

[23] Article 1, GDPR, highlights the need to balance the freedom of data with the fundamental rights of the individuals, especially data protection. Data protection and privacy are also regarded as fundamental rights in Articles 7 and 8 of the European Charter for Fundamental Rights (ECFR), and in Article 8 of the European Charter of Human Rights (ECHR).

[24] American Law Institute (ALI), Restatement of Torts, 2nd, 1977. The reference is to the so-called Prosser's torts, from the Author of the taxonomy, William Prosser: namely, intrusion upon seclusion, disclosure of private facts, appropriation of name or likeness, false light in the public eye.

[25] The difference in terminology between dignitary and data privacy is carefully explained by RC Post, 'Data Privacy and Dignitary Privacy: Google Spain, The Right to Be Forgotten, and The Construction of the Public Sphere' (2018) 67 *Duke Law Journal* 983 ff.

[26] See A Las Casas, *Capitalismo dell'informazione e circolazione della ricchezza. Modelli giuridici statunitensi* (Edizioni Scientifiche Italiane 2024) 37; 57 ff. The commodification of personal data is a well-known process which has caused legal debates regarding data's legal qualification also in civil law systems. See, among others, the pioneering observations formulated by P. Perlingieri, 'L'informazione come bene giuridico' (1990) 2 *Rass. dir. civ.* 329 ff.; C. Camardi, 'Mercato delle informazioni e privacy. Riflessioni generali sulla l. 675/1996' (1998) 4 *Eur. dir. priv.* 1049 ff. More recently, on the same matter, S Sica and V D'Antonio, 'La commodification dei dati personali nella data driven society' in P Stanzione (ed), *I poteri privati delle piattaforme e le nuove frontiere della privacy* (Giappichelli 2022) 129 ff; G Resta, 'The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives' (2011) 26 *Tul. Eur. and Civil Law Forum* 33 ff.

[27] Article VI, § 2, US Constitution. On explicit and implicit pre-emption, JCP Goldberg and BC Zipursky, *Torts* (Aspen Publishers 2010) 389-393. With specific reference to privacy, see PM Schwartz, 'Preemption and Privacy' (2009) 118 *Yale Law Journal* 902 ff.

comprehensive – for example, the California Consumer Privacy Act (CCPA), which governs the processing of consumer data in general – while federal privacy laws are sectorial. However, when federal law applies, it takes precedence over state law. Moreover, since the processing of personal data is a transborder activity, state law is inadequate to properly address it. The same company normally processes the data of users located in different areas of the country, thus exceeding the territorial competence of state lawmakers.

This can create legal gaps. There has been a growing call for a comprehensive privacy and data protection act, with some proposals being advanced, but not yet implemented.[28] Moreover, the increasing multiplication and overabundance of statutory laws causes inconsistencies in judicial decisions. When class actions in the field of data privacy are proposed, they often involve citizens of different states. Frequently, their claims are gathered together, under the system of Multidistrict Litigation (MDL).[29] Normally, in these cases, sectorial federal law applies to all the plaintiffs, while different subclasses of litigants can invoke their own state privacy laws, which are usually broader in material and subjective scope. This fragments the enforcement of data privacy and creates double standards of protection.

Moreover, to start a claim, plaintiffs need to have a 'private right of action' or 'cause of action', granted to them by either common law or statutory law. Individuals lack a general cause of action for ensuring their data privacy.[30] Some federal statutes, such as the Health Insurance Portability and Accountability Act (HIPAA), concerning health data, or the Federal Trade Commission Act (FTCA), are only enforced by the competent authority, the Federal Trade Commission (FTC), as they do not provide for a private right of action.[31] This means that their enforcement is exclusively public. Some others, such as the Electronic Communications Privacy Act (ECPA), or the Fair Credit Reporting Act (FCRA), provide for a cause of action, as well as nominal or statutory damages. Nominal damages exonerate users from the burden of proving their loss, compensation stemming from the mere intentional or negligent breach of the law. Nonetheless, again, these statutes are sectorial (only devoted to the financial sector; or to electronic communications; and so forth), thus their application is limited.

[28] For instance, through the proposal of an American Privacy Rights Act (APRA), on which see the Congressional Research Service report, The American Privacy Rights Act, available at: https://crsreports.congress.gov/product/pdf/LSB/LSB11161.

[29] For an overview of the multi-district litigation mechanism, see J Dodge, 'Facilitative Judging: Organizational Design in Mass Multidistrict Litigation' (2014) 64 *Emory Law Journal* 329 ff.; N Trocker, 'La class action negli Stati Uniti: lo stato dell'arte' (2020) 2 *Rivista di Diritto Processuale* 754 ff.

[30] L Scholz, 'Private Rights of Action in Privacy Law' (2022) 63 *William & Mary Law Review* 1639 ff.

[31] W Hartzog and DJ Solove, 'The FTC and the New Common Law of Privacy' (2014) 114 *Columbia Law Review* 583 ff. For an overview of the legal framework surrounding privacy and how this impacts the perception of privacy as a social value, see S Mazzurco, 'Privacy Law's Role in an Information Economy' (2024) 46 *Cardozo Law Rev.* 123 ff.

The privacy torts provide for a cause of action in this field but, again, they are mostly referred to the idea of dignitary privacy, as the protection of someone's personal and private spheres. Consequently, scholars have pointed out that privacy torts are not particularly well-suited for data privacy, and even more for aggregate litigation, as it will be addressed in greater detail in Section 3 of this essay.[32]

For instance, privacy torts are shaped on an individual basis, which does not correspond to the massive scale of personal data collection on the Internet. They are dependent on intent, and related to damage to personality, which is difficult to demonstrate on a mass scale (for example, when a data breach occurs, or when user data is unlawfully traded to third parties). Eventually, and more strikingly, the torts of invasion of privacy concern the exposure of someone's private information to the public: they require an actual, uninvited, gaze. Conversely, the unlawful collection of user data very seldomly causes harm to the interests in honor or reputation. Rather, it affects more the collective interest in a fair data-driven economy, where human dignity and all the fundamental rights of individuals shall be respected, and where individual self-determination is ensured.

Therefore, collective judicial proceedings in the field of data privacy are normally brought forward through other torts (such as negligence, or even trespass and battery), and contract law (especially, breach of contract for violations of privacy policies). There is also a quest for applying fiduciary law to these disputes.[33] Even with all the uncertainties regarding the applicability of common law remedies to the protection of personal data, class actions remain an efficient and vibrant procedural tool in this field, allowing the needs and claims of groups of individuals to be gathered in court, and performing deterrence against unlawful conducts of defendants. The integrated role of public and private enforcement, and the large class action settlements adopted in these disputes, have led to a growing body of soft law norms and good practices.

Meanwhile, the European GDPR ensures that data subjects have an effective judicial remedy every time their rights are infringed, attributing to them a general cause of action, in Article 79. The Regulation fits into most civil law systems, where individuals can invoke their *personality rights* or *droits de la personalité* in courts. Consequently, if a data subject proves to have suffered harm to their right to data protection, he or she can be eligible for redress (Article 82, GDPR).

Notwithstanding, one of the main weaknesses of the EU legal framework has been the lack of effectiveness of the private enforcement system, especially collective redress, at least until now. The skepticism towards collective private

[32] DK Citron and DJ Solove, 'Privacy Harms' (2022) 102 *Boston University Law Review* 793 ff.

[33] See W Hartzog and N Richards, 'Legislating Data Loyalty' (2022) *Notre Dame Law Review Reflection* 356 ff.; WW Hartzog and N Richards, 'The Surprising Virtues of Data Loyalty' (2022) 71 *Emory Law Journal* 985 ff.; JM Balkin, 'The Fiduciary Model of Privacy' (2020) 133 *Harvard Law Review Forum* 11 ff.; JM Balkin, 'Fixing Social Media's Grand Bargain' (2018) *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper* 11 ff. On the application of fiduciary duties on platforms, in Italian legal literature, V Conte, *Comunicare per contratto* (Edizioni Scientifiche Italiane 2024).

enforcement in Europe can be traced back mainly to cultural and societal reasons, and to the idea of the right of action as inevitably connected to the individual; to procedural law norms on *res judicata,* and to the interpretation of the constitutional right to defense; to the lack of a general EU competence in procedural law; to the conception of the right to data protection as a 'subjective right', shaped on an individual basis[34].

This situation might change in the future, thanks to the newest European digital laws, such as the Data Governance Act and the Data Act, which increasingly reflect a collective dimension of data protection, focusing more on data governance rather than on control over personal data. Moreover, the GDPR itself includes a legal basis for representative actions (namely, Article 80), as acknowledged by the Court of Justice[35].

The Court of Justice, with case *UI v. Osterreichische Post AG*, has also opened the doors to the compensation of non-material damage for unlawful processing of personal data regardless of the seriousness of the harm suffered by the data subject.[36] This new interpretation will be central for collective privacy litigation, as collective claims are aimed precisely at enabling the aggregation of small claims, even when they look trivial on an individual scale. It is along the lines of this approach that legal systems like the German one, which are normally more restrictive in compensating non-pecuniary harms, have welcomed actions such as

[34] In general, the GDPR seems to be constructed around the grounds and foundations of private autonomy and informational self-determination. Both are, however, nowadays, inevitably shaking, in the new consumer relationships. On this matter, in general terms, G Villanacci, 'Autonomia privata e buona fede nella complessa relazione evolutiva con la normativa consumeristica' (2013) 4 *Contratto e impresa* 917 ff.

[35] CJEU, case C-319/20, *Meta Platforms Ireland Ltd v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* [2022].

[36] See the landmark case CJEU, Case C-300/21, *U.I. c. Österreichische Post AG.* The case has been commented widely by authoritative scholarship. Among the various Authors, see C Camardi, 'Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea' (2023) *Nuova giurisprudenza civile commentata* 1136 ff; A Palmieri and R Pardolesi, 'Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)' (2023) IV *Foro Italiano* 268 ff.; S Pagliantini, 'Un altro palcoscenico della "guerra" tra le corti: il danno (immateriale) bagatellare dell'art. 82 GDPR' (2023) IV *Foro Italiano* 268 ff.; M Federico, '"La tempesta perfetta": ultime dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva' (2023) IV *Foro Italiano* 268 ff; U Salanitro, 'Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia' (2023) 3 *Rivista di diritto civile* 426 ff; C Scognamiglio, 'Danno e risarcimento nel sistema del RGPD: un primo nucleo di disciplina eurounitaria della responsabilità civile?' (2023) 5 *Nuova giurisprudenza civile commentata* 1150 ff.; F Episcopo, 'UI v Österreichische Post – A First Brick in the Wall for a European Interpretation of Art 82 GDPR' (2024) 13 *Journal of European Market and Consumer Law* 87 ff. In general, on non-material damages for unlawful processing of personal data, see R Caterina and S Thobani, 'Il diritto al risarcimento dei danni' (2019) 12 *Giurisprudenza italiana* 2805 ff. Recently, see M Faccioli, 'La responsabilità civile per illecito trattamento dei dati personali' in R Bocchini (ed), *Trattato Le piattaforme digitali e-Agorà* (Giappichelli 2025) 896 ff.

the one started in front of the BGH, in November 2024.[37]

Overall, it can be affirmed that substantive law seems to ensure stronger protection to data subjects in Europe, compared to the US, while procedural law seems rather stronger in the US than in Europe. As anticipated, in fact, the role of Rule 23 FRCP in enforcing data privacy is established and essential. This is not surprising. American society is traditionally more reliant on individuals and plaintiffs' initiatives, rather than on the public system. The FTC mostly enforces consumer privacy on the basis of antitrust law and upholds market interests, not to mention that its resources are limited. Also, public enforcement ensures compliance, but it is not tailored to grant compensation and relief.[38]

However, class actions have recently been 'under attack' by the US Supreme Court. The main challenges for collective privacy litigation are currently the choice of an appropriate cause of action, and the issue of establishing standing to sue for federal claims, according to Article III of the US Constitution. This tendency aligns with a general mistrust towards class actions, expressed in Supreme Court rulings such as *Varela*, *Italian Colors Restaurant,* and *Dukes*.[39]

3. In search of the right cause of action for addressing privacy harms

An empirical analysis of US collective privacy litigation shows that the main cases when class actions have been proposed so far are: data breaches, unlawful processing of personal data without users' consent or another valid legal basis, and unauthorized transmission of personal data to third parties. Another distinctive feature of these class actions is that they usually do not end with a judicial decision,

[37] On this line, see already the cases *Schufa*, OLG Hamburg - 13 U 11/24; and BGH - VI ZR 10/24, the Facebook Data Breach referred to in n. 10.

[38] From a critical perspective AE Waldman, *Industry Unbound: The Inside History of Privacy, Data, and Corporate Power* (Cambridge University Press 2021). For some considerations on the law's role in shaping big tech's power, see K Pistor, *The Code of Capital: How the Law Creates Wealth and Inequality* (Princeton University Press 2019); J Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

[39] JE Cohen, 'Law for the Platform Economy' (2017) 51 *UC Davis Law Review* 177-183; more extensively, JJE Cohen, 'Information Privacy Litigation as Bellwether for Institutional Change' (2017) 67 *DePaul Law Review,* 35 ff. Some of the rulings where the Supreme Court is said to have been particularly restrictive towards class actions are: *Stolt-Nielsen S.A. et al. v. Animalfeeds Int'l Corp.*, 559 US 662 (2010); *AT&T Mobility LLC. v. Concepcion*, 563 US 333 (2011); *American Express Co. v. Italian Colors Restaurant*, 570 US 228 (2013); *Epic Systems Inc. v. Lewis et al.*, 138 US 1612 (2018); *Lamps Plus, Inc. v. Varela*, 587 US (2019); *Wal-Mart v. Dukes*, 564 US 338 (2011); *Jennings v. Rodriguez*, 138 S. Ct. 830 (2018). On the topic, J Coffee and A Lahav, 'Class Actions in the Era of Trump: Trends and Developments in Class Certification and Related Issues' (2017) 3 ff available at: https://scholarship.law.columbia.edu/faculty_scholarship/2055; in a comparative perspective, A Palmieri, 'Consumatori, tutela collettiva, arbitrato: di miti (americani) infranti e timidi risvegli (europei)' in CA D'Alessandro and C Marchese (eds), *Ius dicere in a globalized world* (RomaTre-Press 2018) 637 ff.

but with a settlement, where parties agree to a joint solution to their controversy.[40]

In the past few years, plaintiffs have tested in courts more than 80 causes of action. Some class actions have been proposed through federal and state statutory laws (particularly, the Electronic Communications Privacy Act, ECPA, the Stored Communications Act, SCA, and the Telephone Consumer Protection Act, TCPA); others via negligence, trespass, invasion of privacy, unjust enrichment, and breach of contract. Among state laws, California's generally seem to be the most liberal: for example, a private right of action is laid down in both the California Consumer Privacy Act (CCPA) and the Comprehensive Computer Data Access and Fraud Act (CDAFA). These laws often provide also for statutory damages, entitling plaintiffs to receive compensation irrespective of showing actual damage, once the unlawful negligent or intentional conduct is ascertained.

While the provision of statutory damages was sometimes regarded sufficient to establish standing to sue, this orientation has recently been curtailed by the Supreme Court, in the rulings *Spokeo v. Robins* and *TransUnion LLP v. Ramirez*[41].

As anticipated, Article III of the American Constitution requires standing to sue in order to bring an action in court. Standing can be defined as an interest in a case which makes it adversarial. In recent years, the requirements for standing to sue have become more and more restrictive: courts have declared that plaintiffs must prove to have suffered an actual, particularized, and real harm for their action not to be dismissed[42]. In fact, the Supreme Court has recently tightened the loopholes for establishing standing to sue, especially when class actions are proposed for non-material privacy harms. Specifically, the Court has called for a 'stricter' application of the requirement of the 'concreteness' of the harm[43].

Privacy harms are mostly non-material: the consequences of unlawful data processing on a vast scale are emotional distress, anxiety, anguish stemming from the risk of future identity theft, fear of impact on self-determination, and possible discrimination arising from group profiling. In *Spokeo v. Robins* and *TransUnion LLP v. Ramirez,* the Supreme Court highlighted the necessity of establishing the concreteness of this type of harm to obtain redress, even when the enforced legal acts, such as the FCRA, already provide for statutory damages. Some scholars have pointed out that, accordingly, potential 'risks of harm', deriving from 'increased vulnerability to data-driven predictive profiling', might appear too remote and speculative to count as an actionable injury.[44] The Court's judgments are problematic because they tend to deny the relevance of non-material harm in

[40] For an overview of the system of the US case law, Federico, *Protezione dei dati personali* (n 16) 230 ff.

[41] *Spokeo, Inc. v. Robins,* 578 US (2016); *TransUnion LLC v. Ramirez,* 594 US (2021).

[42] *Spokeo, Inc. v. Robins,* cit.

[43] On privacy harms, see I Cofone, *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge University Press 2023).

[44] DJ Solove and DK Citron, 'Standing and Privacy Harms: A Critique of TransUnion v. Ramirez' (2021) 101 *Boston University Law Review* 62 ff.

relation to data privacy interests, while, conversely, privacy torts were formulated exactly for addressing this kind of emotional distress. The rulings also neglect the societal dimension of such harm. Therefore, the main obstacle to collective privacy litigation is to establish standing to sue for redressing privacy harms, often regarded as 'too intangible'.

However, it is quite a blind conception of harm to attribute 'tangibility' only to harms to proprietary interests, while neglecting it for interests such as privacy and data protection[45]. When consumer trust is violated, groups of individuals are discriminated against, or erroneously profiled, there is not merely a risk of harm. Rather, it is real (often, non-material) harm the class is suffering, to their interest in governance and protection of their data.

This situation looks quite paradoxical from a comparative perspective. The US Supreme Court has established a sort of gravity threshold for privacy harms, which needs to be overcome for class actions to be declared admissible. This occurs within a legal context that allows for both statutory and punitive damages. Instead, across the Atlantic, the Court of Justice does not require a certain seriousness for privacy harms to be compensable, establishing that any non-material harm to data protection or privacy is sufficient to bring an action in court. Thus, while American courts seem to be trying to close the doors to class actions in the field of privacy, in Europe, perhaps, these doors may be slowly opening.

Nevertheless, class actions are too enshrined and entrenched in American culture to be so easily defeated. Collective privacy litigation is still vibrant and alive, and plaintiffs are accordingly experimenting with judicial techniques to establish standing to sue in privacy law controversies. A comprehensive statute providing for a general cause of action for infringements of privacy would probably be the most desirable solution, but its adoption is currently unlikely. Hence, the need to explore common law remedies.[46]

Traditionally, privacy has been protected by the four, above-mentioned, privacy torts: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of name or likeness. However, the torts of invasion of privacy address more dignitary than data privacy concerns. They indeed pertain to the protection of the personality and the integrity of someone's image. They aim to protect the individual from unwanted intrusions of their private sphere or from the disclosure of relevant and reserved information to the public. Moreover, the possible damages arising from the infringement of the right to dignitary privacy are often too individualized and specifically connected with an individual's state of affairs to be brought via class actions. Common questions of fact and law should take precedence over individual ones in class actions, according to the

[45] B Chao, 'Privacy Losses as Wrongful Gains' (2021) 106 *Iowa Law Review,* 556 ff.

[46] And, especially, tort law. In the US, indeed, the protection of what in Europe are addressed to as the 'rights to personality' is assigned to the law of torts. See JA Page, 'American Tort Law and the Right to Privacy' in G Brüggemeier, A Colombi Ciacchi and P O'Callaghan (eds), *Personality Rights in European Tort Law* (Cambridge University Press 2010), 38 ff.

requirement of 'predominance', Rule 23(b)(3).

Meanwhile, data privacy is more about individual control over the dissemination of their data, and the quest for online anonymity. In cases of unlawful personal data processing, when personal data are collected in violation of US laws, the impact on a person's identity is generally limited. Conversely, unlawful practices by data collectors can significantly undermine informational self-determination, often on a vast scale.

Looking at the specifics of the four privacy torts allows to further confirm their unsuitability for class actions.[47] *(i)* The tort of false light in the public eye requires the information disseminated to be 'highly offensive', and the offender to have 'actual malice', circumstances which are specific and typical to certain individuals, and difficult to prove with reference to a whole class. *(ii)* Intrusion upon seclusion requires the intrusion to be 'highly offensive' and the defendant's conduct to be 'intentional'. However, the high relevance of the offense is hard to prove, especially in a context where privacy harm is often said to lack concreteness.[48] *(iii)* Public disclosure of private fact, known as the right of publicity, also requires the conduct to be highly offensive. This model is not well-suited for the disclosure of personal data for commercial reasons, which in most cases is not offensive; nor for the undue processing of personal data regardless of someone's consent. *(iv)* Eventually, the tort of appropriation requires the defendant to unduly take actual advantage of the use of someone's name or image. This tort seems to be the most coherent with the commercial value of users' data, and able to tackle the undue benefits that defendants might derive from data exploitation, perhaps being the most adaptable to the data-driven economy.[49] Nevertheless, the tort also proves to be unsuitable for data privacy infringements which do not involve identity theft, or misuse of personal data.

Contract law has also been applied to induce companies to respect their privacy policies. Accordingly, the breach of a privacy policy is compared to a breach of contract. However, contract law may also prove insufficient for redressing privacy harms. To begin with, privacy policies *per se* may cause asymmetries between parties, when they provide for the possibility to process users' data regardless of their valid, informed, specific, consent.[50] Thus, enforcing these policies would not necessarily ensure individual rights. Additionally, in data breaches, it might be difficult to prove causation. Data breach injuries (identity thefts; frauds; costs to be taken in order to safeguard data after the breach) are hard to trace to a defendant's specific breach of terms of services, or privacy policies.[51] Moreover, when there are no terms of service, or when they are ambiguous and incomplete,

[47] See Las Casas (n 25) 57 ff. On privacy torts and data collection, DK Citron, 'Mainstreaming Privacy Torts' (2010) 98 *California Law Review* 1824 ff.
[48] WL Prosser, 'Privacy' (1960) 48 *California Law Review,* 383 ff.
[49] Las Casas (n 25) 58.
[50] Las Casas (n 25) 118 ff.
[51] Chao (n 46) 558 ff.

users are left without protection. Furthermore, it has also been argued that the lack of awareness and acceptance of users of terms and conditions strips the consideration requirements from these terms, which makes it difficult to treat them as enforceable contracts.[52]

Moreover, in contract law, recovery for 'emotional disturbance' is generally excluded, unless the breach caused also bodily harm, or it 'is of such a kind that serious emotional disturbance was a particularly likely result'[53]. While it can be 'likely' that, if certain technical and organizational measures are not adopted, data breaches or data protection infringements will occur, the seriousness of the emotional disturbance might be harder to prove, especially with courts continuing to overlook the societal dimension of privacy harms.

This corroborates the need to elaborate on other plausible causes of action, which may prove more effective in ensuring data privacy, beyond contract law and specific statutory norms. Following the paths that courts have traced, some remedies worth exploring are unjust enrichment and the tort of negligence.

Unjust enrichment relates to profits gained by the defendant from the processing of users' data and its commercial value.[54] It is often used as an ancillary remedy, alongside tort or contract claims. This is possible in the US legal system, where unjust enrichment is not strictly a subsidiary remedy, unlike, for instance, in Italy.

A second interesting option is to expand the tort of negligence to allow compensation for unlawful personal data processing. This tort requires a duty of care, breach of that duty, causation, and damage. A general duty of care to lawfully process user data might be inferred from federal privacy laws. For example, statutes like the HIPAA, even if they do not provide for a cause of action, might be regarded as establishing a duty of care in the processing of health data.[55] The Federal Trade Commission Act might also serve as a basis for such duties, prohibiting unfair or deceptive practices[56]. These laws establish a high standard of care for platforms

[52] Las Casas (n 25) 105 ff.

[53] ALI, Restatement (2nd) of Contracts § 353 (1981).

[54] On the potentials of unjust enrichment, see Las Casas (n 25) 185 ff.; with respect to the European legal system, G Biancardi, 'Il trattamento dei dati personali nel prisma dell'ingiustificato arricchimento' (2024) 4-5 *Il Diritto dell'Informazione e dell'Informatica,* 641 ff. In general, from a comparative perspective, see P Pardolesi, *Arricchimento da fatto illecito: i rimedi. Dai disgorgement damages alla retroversione degli utili* (Cacucci 2023). A remedial tool similar to unjust enrichment, but recently trialed by public authorities, and specifically by the FTC, is 'algorithmic disgorgement'. Algorithmic disgorgement or 'model deletion' consists of the restitution of profits unduly gained by Big Tech while also forcing them to delete users' data used to train their algorithms. On algorithmic disgorgement, TC Li, 'Algorithmic Destruction' (2022) 75 *SMU Law Review* 479; J Hutson and B Winters, 'America's Next "Stop Model!": Model Deletion' (2024) *Georgia Law Technology Review* 124 ff.

[55] DJ Solove, 'Lawsuits for HIPAA Violations and Beyond: A Journey Down the Rabbit Hole' (2014) *TeachPrivacy* available at: https://teachprivacy.com/lawsuits-hipaa-violations-beyond-journey-rabbit-hole/.

[56] Those are often used to tackle data privacy violations in the US as well as, increasingly, in Europe. On unfair commercial practices and consumer law see, among the others, R Caterina, 'Pratiche commerciali scorrette e tutela del consumatore' in *Studi in onore di Aldo Frignani. Nuovi orizzonti del diritto comparato europeo e transnazionale* (Jovene 2011) 123 ff.

and data controllers, who may also be seen as being in proximity to consumers and users whose data they process.

However, the most critical hurdle concerning the tort of negligence remains proving the harm, which must be cognizable and serious enough to meet the burden of proof for redress and compensation, and to admit standing. Traditionally, in actions in negligence, non-pecuniary damages used to be awarded mostly when they were a consequence (primary or secondary) of an injury to a person or property. That is not the case when the trust of individuals is betrayed by Big Tech processing their data. Nevertheless, negligence, which is one of the most flexible torts, has evolved and developed over time, extending its applications to the redress of non-pecuniary harms more broadly, and this is an option worth exploring also for privacy damage.

4. Pushing the boundaries of tort law

Even if we admit the applicability of the tort of negligence in collective privacy cases we would be confronted with the issues of demonstrating the seriousness of the damage suffered, according to the conditions established by the Supreme Court. This problem might be partially resolved through the application on platforms of duties resembling those of fiduciary law. This solution has been suggested by some scholars to delineate a comprehensive set of rules regarding data processing,[57] but it might be beneficial also for the purpose of establishing standing to sue.

Fiduciary law is a complicated scheme that encompasses a wide range of scenarios. It is characterized by the existence of a close relationship between the fiduciaries and their clients, where the latter are in a position of asymmetry and vulnerability, and have expectations of trust, loyalty, and care towards the former.[58] The limited operability of fiduciary law compared to tort or contract law makes it possible not to restrict compensation stemming from their breach to the principles of foreseeability or remoteness. As ruled in the landmark cases *Nocton v. Lord Ashburton* and *Keech v. Sandford*: 'The high duty assumed and the difficulty of detecting such breaches make it fair and practical to adopt a measure of compensation calculated to ensure that fiduciaries are kept up to their duty'[59].

[57] See the references in n. 33.

[58] L Smith, *The Law of Loyalty* (Oxford 2023); LI Rotman, 'Understanding Fiduciary Duties and Relationship Fiduciarity' (2017) 62 *McGill Law Journal* 977; W Bradley Wendel, 'Fiduciary Law' in AS Gold, JCP Goldberg, DB Kelly, E Sherwin and HE Smith (eds), *The Oxford Handbook of the New Private Law* (Oxford University Press 2020) 312-323. In general, on the concept and theories of security and trust in patrimonial relationships, beyond fiduciary law, F Manolita, *Sicurezza, fiducia e razionalità nei rapporti patrimoniali* (Edizioni Scientifiche Italiane 2022).

[59] On the cases, in more detail, see Rotman (n 59) passim.

Fiduciary law has been applied when protection offered by tort, contract or unjust enrichment law was absent.[60]

The flexibility of fiduciary law in the common law system has led some authors to assimilate platforms to 'information' fiduciaries, having a duty to protect their users from loss of control of their data. Jack Balkin has proposed to offer platforms a 'grand bargain': big tech companies would be able to benefit from the liability exemptions that they currently enjoy on the Internet (according to Sections 230 and 520, Communications Decency Act, CDA, and Digital Millennium Copyright Act, DMCA), if they accept being subjected to fiduciary duties.[61]

The main advantage of this theory is that it would impose a comprehensive set of duties on platforms. Furthermore, according to the 2nd Restatement of Torts, the right to receive compensation arises directly from the breach of a fiduciary duty.[62] Therefore, there would be no need to prove standing, or an actual and individualized harm, to bring an action in US courts.

Fiduciary law has also entered civil law systems, including Italy and Germany, with respect to the law of trusts and different relational schemes.[63] Among its various applications and similarities with other civil law institutions, like the contract of mandate or, naturally, trust, fiduciary law resembles the Italian and German (controversial) doctrines of the 'social contact' (*contatto sociale* or *sozialer Kontakt)*. The 'social contact' is characterized by one party placing reliance and trust on the other. In cases of damage, the obligation to redress arises precisely from the 'qualified relationship' between the parties. Accordingly, those parties that are not formally bound by a contract, but have a close and qualified relationship, are linked by an obligation 'of protection' (*obblighi di protezione senza prestazione*). In Italy, this theory is grounded in the concept of good faith in private law relations (among others, see articles 1175 and 1375 c.c.). However, the social contact doctrine has been criticized for its uncertainty and undue expansion, and because of the lack of a specific legal ground at the expense of tort law.[64]

Moreover, there is one main critical point concerning the application of fiduciary duties on platforms. Fiduciary relations have to be *qualified:* they are mostly one-to-one, which makes it difficult to adapt them to a setting where

[60] *Keech v Sandford* [1726] EWHC J76; *Nocton v Lord Ashburton* [1914] AC 932. See LI Rotman, 'Fiduciary Law's 'Holy Grail': Reconciling Theory and Practice in Fiduciary Jurisprudence' (2011) 91 *Boston Univ. Law Rev* 921-936.

[61] JM Balkin, 'Fixing Social Media's Grand Bargain' 1-20.

[62] Restatement 2nd of Torts, §874.

[63] For a comparative overview, T Kuntz, 'Spaces and Elements' in S Davis, T Kuntz and G Shaffer (eds), *Transnational Fiduciary Law* (Cambridge University Press 2023) 37 ff.

[64] On the matter, see CW Canaris, 'Il contatto sociale nell'ordinamento giuridico tedesco' (2017) *Rivista di diritto civile*, 1 ff.; K Larenz, *Lehrbuch des Schuldrechts*, I, *Allgemeiner Teil* (C.H. Beck 1982); A Procida Mirabelli Di Lauro, 'L'obbligazione come rapporto complesso' (2018) *Rivista di diritto civile* 917; A Zaccaria, 'La resistibile ascesa del contatto sociale' (2013) *Rivista di diritto civile* 77 ff.; L Mengoni, 'Responsabilità contrattuale (dir. vig.)' *Enciclopedia del diritto* (Giuffrè 1988) 1072-1099; C Castronovo, 'Obblighi di protezione' in *Enciclopedia giuridica* (Treccani 1990) 1ff.

platforms act towards their users through standardized contracts and on a mass scale. Furthermore, it would be difficult to maintain the existence of a fiduciary relationship between data subjects and third parties who collect personal data not directly from users. Let's think, for instance, about data brokers: they collect data without users' active consent, often through web-scraping. Users can opt out of these activities, yet it is difficult to argue that there is a fiduciary relationship between the data broker and the indefinite mass of consumers whose data are gathered. In order for a relationship of trust to exist, trust needs to have strong grounds.[65]

Given these conceptual limitations, another viable option might be adapting and rethinking the tort of negligence to meet the demands of the digital age. For instance, a possibility might be reversing the burden of proof, thus shifting to a model of 'reinforced' accountability, similar to the European GDPR.

After all, law has to change in a society that changes, and the same goes for tort law, in response to the development of new technologies. In this sense, American tort law has historically been flexible and adaptable to the extraordinary changes and developments experienced by the US economy.[66] American courts have imposed restrictions or expansions on the scope of liability, linked to the need to support emerging industries, or to the need to protect victims.[67] Naturally, there cannot be liability without harm. But damage may also arise in the shape of societal harm, and this new dimension of wrongs should not be ignored or neglected.

When confronted with technological innovations, American courts have questioned the fault principle as the basis of tort law, and have then elaborated the different, yet related, frameworks of strict and later enterprise liability, for activities performed on a large scale and bringing innovations to society, increasing risks of damage and injuries.[68] Those features are also present with respect to personal data processing.

Yet, the strict liability paradigm looks adequate with respect to data leaks, but less for cases involving unlawful processing of personal data. It may also prove to be too severe and not so practically feasible with respect to activities that are

[65] An interesting assessment of the theory of the information fiduciaries is drafted by DM Filler, DM Haendler and JL Fischer, 'Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data' (2022) 54 *Connecticut Law Review* 105 ff.

[66] G Alpa, 'Responsabilità civile (profili di diritto comparato)' in *I tematici – Responsabilità civile*, ed by C Scognamiglio, *Enciclopedia del diritto* (Giuffrè 2024) 749.

[67] This has been performed especially with reference to product liability, giving rise to strict liability schemes. On the topic, see CC Tilley, 'Just Strict Liability' (2022) 43 *Cardozo Law Review* 2317 ff. On enterprise liability theories which also developed during the period of the second industrial revolution, see G Keating, 'The theory of enterprise liability and common law strict liability' (2001) 54 *Vanderbilt Law Review* 1292-1333.

[68] The landmark case for strict liability regimes is *Rylands v. Fletcher* [1868] (H.L.). On strict liability and its implications in terms of justice aims, GC Keating, 'Distributive and Corrective Justice in the Tort Law of Accidents' (2000) 74 *Southern Cal. Law Review* 193 ff.

now very widespread and involve actors that are considerably different from one another. In fact, one thing is when personal data are processed by gatekeepers, and another is when they are processed by small data controllers, such as small enterprises, on which strict liability may be too burdensome. These could also argue that their economic activity would be unduly hampered by the threat of tort liability. Thus, another option might be to increase the due diligence standards on negligence-based liability and reverse the burden of proof on defendants.

Whether expanding the role of the tort of negligence is feasible, lowering the standard of the burden of proof for plaintiffs, as well as conferring concreteness to data privacy harm beyond its mere individual dimension, depends on the function that we attribute to tort law.[69] If we attribute to tort law not only a restorative function, but also a corrective and punitive one, then we cannot avoid conferring on the social dimension of privacy harm appropriate relevance. If we assign a regulatory function and a distributive justice purpose to tort law, it would then follow that it could and should perform deterrence towards unfair and unlawful practices, imposing the cost of innovation on the companies that are able to bear it. Wrongs and torts shall be examined not only from an individual perspective, but also from a social one; and the costs of those wrongs shall be spread on those who benefit from the 'dangerous' activities that they perform.

Accordingly, it may be desirable that American courts delineate a parallel and different system of tort law and liability in relation to data privacy offenses, in the upcoming years. In this sense, the European model might be an appropriate and useful point of reference, looking at the standards and the interpretation of Article 82, GDPR. Civil liability for unlawful personal data processing is now a peculiar and special system in Europe, with its own rules, laid down by the

[69] The functions of tort law have been widely debated and discussed. On this topic, see PG Monateri, 'Responsabilità civile nel diritto comparato' in *Digesto delle discipline privatistiche – Sezione civile* (1998) 12 ff.; A Procida Mirabelli di Lauro, *La responsabilità civile. Strutture e funzioni* (Giappichelli 2004); U Magnus, 'Tort Law in General' in JM Smits (ed), *Elgar Encyclopedia of Comparative Law* (Edward Elgar 2006); Goldberg and Zipursky, *Torts*; S Grundmann, HW Micklitz and M Renner, *New Private Law Theory: A Pluralist Approach* (Cambridge University Press 2021) 272 ff.; A Ripstein, 'Theories of the Common Law of Torts' in *Stanford Encyclopedia of Philosophy* (2022) https://plato.stanford.edu/entries/tort-theories/; G Alpa, (n 65) 776 ff. On the law and economics approach to civil liability, inaugurating the tendency of considering the interactions between law and other social sciences' disciplines, see the historic works of R Pound, 'The Economic Interpretation of the Law of Torts' (1940) 53(3) *Harvard Law Review* 365 ff.; F James, 'Social Insurance and Tort Liability' (1952) 27 *NYU Law Review* 537; RH Coase, 'The Problem of Social Cost' (1960) 3 *The Journal of Law and Economics* 1 ff.; G Calabresi, 'Some Thoughts on Risk Distribution and the Law of Torts' (1961) 70(4) *Yale Law Journal* 499 ff.; in Italian literature, P Trimarchi, 'Sul significato economico dei criteri di responsabilità contrattuale' (1970) *Riv. trim. dir. proc. civ.* 512 ff.; U Mattei and R Pardolesi, 'Law and economics in civil law countries: a comparative approach' (1991) 11 265 ff.; R Pardolesi and A Arcuri, 'Analisi economica del diritto', in *Enciclopedia del diritto, Agg.*, VI (Giuffrè 2002) 7 ff. See an overview of the debate in: R Caterina, 'Comparative Law and Economics' in JM Smits (ed), *Elgar Encyclopedia of Comparative Law* (Edward Elgar Publishing 2006) 161–171.

GDPR, further concretized by the Court of Justice. The system of liability is completed and complemented by the principle of accountability, which imposes due diligence obligations on data controllers. Those obligations extend beyond mere compliance, defining and shaping a reinforced standard of care for data controllers, to be considered also when establishing liability.[70]

In fact, it is true that, on the one hand, common law courts have been reluctant to expand the domain of strict liability.[71] But, on the other hand, courts have also gradually inserted elements of strict liability in negligence claims over time.[72] One example is 'presumptive liability' which shifts the burden of proof to defendants, placing them in charge of providing evidence to escape liability in trials.[73] Accordingly, this technique locates 'between the two extremes of: *i*) a negligence standard that might leave plaintiffs without relief for legitimate harms where they lacked affirmative evidence, *ii*) an unsought strict liability standard that might saddle businesses with over-burdensome litigation costs'.[74] The resulting regime would be similar to the Italian scheme of liability for hazardous activities, under Article 2050 of the Italian civil code, as well as to the German vicarious liability, under Paragraphs 831 and 832 of the *Bürgerliches Gesetzbuch*.

From this perspective, a new federal privacy law would not create another tort or remedy, but would give individuals the private right of action to act under existing ones. Expanding the tort of negligence, and completing it with accountability and with a reversal of the burden of proof, would also acknowledge the relevance of the societal dimension of data privacy harms. If strict liability might be too onerous on companies, especially for privacy harms, which do not normally represent a threat to the security and life of individuals – unlike the scheme adopted for product liability in the twentieth century – a uniform, reinforced standard of care for data controllers would perhaps partially rebalance the power asymmetries between companies and digital users in the platform economy.

This issue extends beyond privacy harms. It touches broadly upon the role of tort law in our society. Tort law should address market and technological innovations, navigating the challenges of regulating the economy, and ensuring the protection of weaker parties in society, while avoiding overly restrictive regimes.[75] A recalibrated tort law framework, sensitive to the collective and diffuse nature of digital harms, represents, therefore, a legal necessity.

[70] On the risk-based approach and the accountability principle, see R Carleo, 'Il principio di accountability nel GDPR: dalla regola alla auto-regolazione' (2021) 1 *Nuovo diritto civile* 359 ff.; S. Sica, V. D'Antonio, G. Giannone Codiglione and G. Sciancalepore, 'Privacy, tutela del consumatore e risk based approach' *Comparazione e diritto civile* 1-21.

[71] M Bussani, AJ Sebok and M Infantino, *Common and Civil Law Perspectives on Tort Law* (Oxford University Press 2022) 48.

[72] JCP Goldberg and BC Zipursky, 'The Strict Liability in Fault and the Fault in Strict Liability' (2016) 85 *Fordham Law Review* 744-786.

[73] M Bussani, AJ Sebok and M Infantino, (n 70) 45.

[74] M Bussani, AJ Sebok and M Infantino, (n 70) 46.

[75] On the role of private law remedies as a regulatory tool, A Zoppini, *Il diritto privato e i suoi confini* (Il Mulino 2020).

5. An emblematic story (not yet over): the *Rodriguez v. Google* class action

In the final part of this writing, the focus shall be put on a dispute still pending in a US District Court, namely on the case *Rodriguez v. Google*[76], one of the several privacy class action suits brought against the leader in the search engine industry. At the stage of the proceedings now reached (in the imminence of the date scheduled for the beginning a federal jury trial), the case offers some important clues on the pivotal role of collective redress actions, and at the same time illustrates the hurdles on the way of achieving a remedy through these procedural devices. The representative plaintiffs initiated a putative class action against the defendant company, accused of engaging in wrongful data practices. Their allegations dealt with the provider's privacy framework; more specifically the practice under scrutiny concerned the 'Web & App Activity' (WAA) and 'supplemental Web & App Activity' (sWAA) buttons, which in theory permit users to control their personal data, but in reality did not prevent the gathering of such data.

After more than three years of preliminary skirmishes, a decisive event occurred in the first days of 2024, when the first instance judge issued an order to certify the proposed classes.[77] With respect to all the three claims that overcame multiple motions to dismiss – 1) invasion of privacy; 2) intrusion upon seclusion; 3) violation of a California statute [the Comprehensive Computer Data Access and Fraud Act (CDAFA)] – the court found that all the prerequisites set out in Rule 23(a) (numerosity; commonality; typicality; adequacy) of the Federal Rules of Civil Procedure were met. That said, the court certified both a Rule 23(b)(3) damages class and a Rule 23(b)(2) injunctive relief class. It is quite interesting to give a quick look at the assessment of the predominance requirement, one of the conditions (the other being 'superiority') that must be satisfied in the framework of Rule 23(b)(3) certification. The analysis is carried out separately: I) for the intrusion upon seclusion and invasion of privacy claims; II) for the CDAFA claim. As to the first ones, the court considers capable of resolution class-wide the core questions to be answered: the existence of a reasonable expectation of privacy;[78]

[76] Case No. 20-cv-4688-RS (N.D. Cal.).

[77] United States District Court for the Northern District of California; order of 3 January 2023 (accessible at https://www.googlewebappactivitylawsuit.com/Home/Documents).

[78] See the above-mentioned order of 3 January 2023: 'the relevant question is whether the members, who shared common conduct, had an objective, reasonable expectation of privacy based on Google's representation about the sWAA button to all members under these claims'. More generally, on this issue, see P Friedl, *Reasonable Expectations of Privacy: With Special Regard to European Privacy and Data Protection Law* (Springer 2025); the Author observes that this concept 'has found support in a great many of jurisdictions and legal environments' (p. 3).

the high degree of intrusion related to the conduct.[79] As to the last claim, all the objections raised by the defendant were deemed to be not well-founded. The classes certified under 23(b)(3) for the invasion of privacy and intrusion upon seclusion claims were subsequently modified,[80] not upsetting the general picture.[81]

After the certification, the defendant moved for summary judgment on all claims advanced by the plaintiffs. The District Court has recently denied the motion.[82]

Among the various issues discussed in the judge's opinion, it is worthy to recall the problem of the nature of the tortfeasor's conduct that may give rise to liability for the invasion of privacy claims. In the light of the established case law of the Federal Courts, this intrusion shall be 'highly offensive' to a reasonable person

[79] According to the above-mentioned order of 3 January 2023, the defendant 'fails to make a case for why these additional questions supersede the central inquiry: whether a reasonable person would find the intrusion by Google highly offensive'. S. Mazzurco 'Privacy Law's Role' (n 30), observes that, in applying privacy torts, 'courts often evaluate whether the invasion would highly offend a reasonable person by looking to the plaintiff's and defendant's role-relationship. In the process, they articulate role-based privacy norms, perhaps informed by a view of existing societal expectations (i.e., role-taking), but importantly, bolstering a particular role-construction with the coercive power of law (i.e., role-making)' (p. 151-2).

[80] United States District Court for the Northern District of California; order of 5 April 2024 (accessible at https://www.googlewebappactivitylawsuit.com/Home/Documents); the defendant's motion to modify the class certification order was granted in part.

[81] The description of the relevant classes can be found at the https://www.googlewebappactivitylawsuit.com/

For the alleged violation of the CDAFA, the classes are the following:

Class 1: All individuals who, during the period beginning July 1, 2016 and continuing through September 23, 2024, (a) had their 'Web & App Activity' and/or 'supplemental Web & App Activity' setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running the Android operating system, because of the Firebase Software Development Kit (SDK) and/or Google Mobile Ads SDK.

Class 2: All individuals who, during the period beginning July 1, 2016 and continuing through September 23, 2024, (a) had their 'Web & App Activity' and/or 'supplemental Web & App Activity' setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running a non-Android operating system, because of the Firebase SDK and/or Google Mobile Ads SDK.

For the alleged invasion of privacy and intrusion upon seclusion legal claims, the classes are the following:

Class 1: All 'non-Enterprise' and 'non-Unicorn' individuals who, during the period beginning July 1, 2016 and continuing September 23, 2024, (a) had their 'Web & App Activity' and/or 'supplemental Web & App Activity' setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running the Android operating system, because of the Firebase Software Development Kit (SDK) and/or Google Mobile Ads SDK.

Class 2: All 'non-Enterprise' and 'non-Unicorn' individuals who, during the period beginning July 1, 2016 and continuing through September 23, 2024, (a) had their 'Web & App Activity' and/or 'supplemental Web & App Activity' setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running a non-Android operating system, because of the Firebase SDK and/or Google Mobile Ads SDK.

[82] United States District Court for the Northern District of California; order of 7 January 2025 (available at https://law.justia.com/cases/federal/district-courts/california/candce/3:202 cv04688/362381/445/).

and unwarranted, so as to constitute an 'egregious breach of social norms'[83]. This outcome seems to be confirmed in the case at stake, by the fact that the defendant collected personal data 'despite concerns raised by its employees and with the knowledge that its disclosures are ambiguous and deficient'.

Regardless of what might happen next, the case above summarized witnesses the continuing vitality of the class action suit and, more broadly, of the collective ligation when applied to privacy issues. And, not surprisingly, notwithstanding all the obstacles, disputes of this kind are gaining room in different contexts. Just to point out one of the situations in which this trend materializes, in June 2024 the Amsterdam Court of Appeal (*Gerechtshof Amsterdam*) gave the green light to a collective action aimed at seeking compensation against two undertakings, with respect to the collection and processing personal data on an extensive level.[84] The road is long and full of rough edges, but it would be a grave mistake to give in to pessimism.

Bibliography

Alpa G., 'Responsabilità civile (profili di diritto comparato)' in *I tematici – Responsabilità civile*, ed by Scognamiglio C., *Enciclopedia del diritto* (Giuffrè 2024) 749; 776 ff.

Balkin J.M., 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) *UC Davis Law Review* 1149 ff.

Balkin J.M., 'Fixing Social Media's Grand Bargain' (2018) *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper* 11 ff.

Balkin J.M., 'The Fiduciary Model of Privacy' (2020) 133 *Harvard Law Review Forum* 11 ff.

Becerril A. 'The value of our personal data in the Big Data and the Internet of all

[83] See, for instance, *In re Facebook, Inc. Internet Tracking Litig.* ('Facebook Tracking'), 956 F.3d 589, 606 (9th Cir. 2020); *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272, 295 (2009)
[84] ECLI:NL:GHAMS:2024:1651.

Things Era' (2018) 7(2) *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal* 71

Biancardi G., 'Il trattamento dei dati personali nel prisma dell'ingiustificato arricchimento' (2024) 4-5 *Il Diritto dell'Informazione e dell'Informatica,* 641 ff.

Bocchini R., 'Nuovi beni digitali e mondi dematerializzati. Il metaverso; New digital goods and dematerialised worlds. The metaverse' (2023) 1 *European Journal of Privacy Law and Technologies* 45-54

Bradford A., *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020)

Bradford A., *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023)

Bueno Biot A., 'La contraprestación en forma de datos personales: el nuevo paradigma en la era digital' (2025) 22 *Actualidad Jurídica Iberoamericana* 1122

Burbank S.B., Farhang S. and Kritzer H.M, 'Private Enforcement' (2013) 17 *Lewis & Clark Law Review* 637, 674

Bussani M., Sebok A.J. and Infantino M., *Common and Civil Law Perspectives on Tort Law* (Oxford University Press 2022)

Calabresi G., 'Some Thoughts on Risk Distribution and the Law of Torts' (1961) 70(4) *Yale Law Journal* 499 ff.

Camardi C., 'Mercato delle informazioni e privacy. Riflessioni generali sulla l. 675/1996' (1998) 4 *Eur. dir. priv.* 1049 ff.

Camardi C., 'Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea' (2023) *Nuova giurisprudenza civile commentata* 1136 ff

Canaris C.W., 'Il contatto sociale nell'ordinamento giuridico tedesco' (2017) *Rivista di diritto civile*, 1 ff.

Carleo R., 'Il principio di accountability nel GDPR: dalla regola alla auto-regolazione' (2021) 1 *Nuovo diritto civile* 359 ff.

Carleo R., 'Piattaforme digitali e contratto – Digital Platforms and Contracts' (2022) 1 *European Journal of Privacy Law and Technology* 76

Carstens A., 'Regulating big tech in the public interest' (2022) 274 *SUERF Policy Brief*

Castronovo C., 'Obblighi di protezione' in *Enciclopedia giuridica* (Treccani 1990) 1 ff.

Caterina R., 'Comparative Law and Economics' in JM Smits (ed), *Elgar Encyclopedia of Comparative Law* (Edward Elgar Publishing 2006) 161–171.

Caterina R., 'Pratiche commerciali scorrette e tutela del consumatore' in *Studi in onore di Aldo Frignani. Nuovi orizzonti del diritto comparato europeo e transnazionale* (Jovene 2011) 123 ff.

Caterina R. and Thobani S., 'Il diritto al risarcimento dei danni' (2019) 12 *Giurisprudenza italiana* 2805 ff.

Chao B., 'Privacy Losses as Wrongful Gains' (2021) 106 *Iowa Law Review,* 556 ff.

Citron D.K. and Solove D.J., 'Privacy Harms' (2022) 102 *Boston University Law Review* 793 ff.

Citron D.K., 'Mainstreaming Privacy Torts' (2010) 98 *California Law Review* 1824 ff.

Coase R.H., 'The Problem of Social Cost' (1960) 3 *The Journal of Law and Economics* 1 ff.

Coffee J. and Lahav A., 'Class Actions in the Era of Trump: Trends and Developments in Class Certification and Related Issues' (2017) 3 ff., available at: https://scholarship.law.columbia.edu/faculty_scholarship/2055

Cofone I., *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge University Press 2023)

Cohen J.E., 'Information Privacy Litigation as Bellwether for Institutional Change' (2017) 67 *DePaul Law Review,* 35 ff.

Cohen J.E, 'Law for the Platform Economy' (2017) 51 *UC Davis Law Review* 177-183

Cohen J.E, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019)

Conte V., *Comunicare per contratto* (Edizioni Scientifiche Italiane 2024)

Dodge J., 'Facilitative Judging: Organizational Design in Mass Multidistrict Litigation' (2014) 64 *Emory Law Journal* 329 ff.

Episcopo F., 'UI v Österreichische Post – A First Brick in the Wall for a European Interpretation of Art 82 GDPR' (2024) 13 *Journal of European Market and Consumer Law* 87 ff.

Faccioli M., 'La responsabilità civile per illecito trattamento dei dati personali' in Bocchini R. (ed), *Trattato Le piattaforme digitali e-Agorà* (Giappichelli 2025) 896 ff.

Federico M., '"La tempesta perfetta": ultime dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva' (2023) IV *Foro Italiano* 268 ff.

Federico M., *Protezione dei dati personali e tutela collettiva. Itinerari di comparazione tra Europa e Stati Uniti* (Giappichelli 2024)

Filler D.M., Haendler D.M. and Fischer J.L., 'Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data' (2022) 54 *Connecticut Law Review* 105 ff.

Finocchiaro G., *Intelligenza artificiale. Quali regole?* (il Mulino 2024)

Friedl P., *Reasonable Expectations of Privacy: With Special Regard to European Privacy and Data Protection Law* (Springer 2025)

Gambacorta L. and Shreeti V,, 'The AI supply chain' (2025) 154 *BIS Working Paper*

Goldberg J.C.P. and Zipursky B.C., *Torts* (Aspen Publishers 2010) 389-393

Goldberg J.C.P. and Zipursky B.C., 'The Strict Liability in Fault and the Fault in Strict Liability' (2016) 85 *Fordham Law Review* 744-786.

Grundmann S., Micklitz H.W. and Renner M., *New Private Law Theory: A Pluralist Approach* (Cambridge University Press 2021) 272 ff.

Hartzog W. and Solove D.J., 'The FTC and the New Common Law of Privacy' (2014) 114 *Columbia Law Review* 583 ff.

Hartzog W. and Richards N, 'Legislating Data Loyalty' (2022) *Notre Dame Law Review Reflection* 356 ff.

Hartzog W. and Richards N., 'The Surprising Virtues of Data Loyalty' (2022) 71 *Emory Law Journal* 985 ff.

Hetcher S., 'Changing the Social Meaning of Privacy in Cyberspace' (2001) 15 *Harv. J.L. & Tech.* 149

James F., 'Social Insurance and Tort Liability' (1952) 27 *NYU Law Review* 537

Kagan R., *Adversarial Legalism: The American Way of Law* (Harvard University Press 2001) 16

Keating G.C., 'Distributive and Corrective Justice in the Tort Law of Accidents' (2000) 74 *Southern Cal. Law Review* 193 ff.

Keating G.C., 'The theory of enterprise liability and common law strict liability' (2001) 54 *Vanderbilt Law Review* 1292-1333

Kuntz T., 'Spaces and Elements' in Davis S., Kuntz T. and Shaffer G. (eds), *Transnational Fiduciary Law* (Cambridge University Press 2023) 37 ff.

Larenz K,, *Lehrbuch des Schuldrechts*, I, *Allgemeiner Teil* (C.H. Beck 1982)

Las Casas A., *Capitalismo dell'informazione e circolazione della ricchezza. Modelli giuridici statunitensi* (Edizioni Scientifiche Italiane 2024)

Lener S.M., 'Personal data as counter-performance in exchange for contents or services after amendments to the Italian Consumer Code' (2024) *Rivista di diritto privato* 135

Li T.C., 'Algorithmic Destruction' (2022) 75 *SMU Law Review* 479; J Hutson and B Winters, 'America's Next "Stop Model!": Model Deletion' (2024) *Georgia Law Technology Review* 124 ff.

Magnus U., 'Tort Law in General' in Smits J.M. (ed), *Elgar Encyclopedia of Comparative Law* (Edward Elgar 2006)

Manolita F., *Sicurezza, fiducia e razionalità nei rapporti patrimoniali* (Edizioni Scientifiche Italiane 2022)

Marciano A., Nicita A. and Ramello G.B., 'Big data and big techs: understanding the value of information in platform capitalism' (2020) 50 *Eur J Law Econ* 345

Mattei U. and Pardolesi R., 'Law and economics in civil law countries: a comparative approach' (1991) 11 265 ff.

Mazzurco S., 'Privacy Law's Role in an Information Economy' (2024) 46 *Cardozo Law Rev.* 123 ff.

Mengoni L., 'Responsabilità contrattuale (dir. vig.)' *Enciclopedia del diritto* (Giuffrè 1988) 1072-1099

Monateri P.G., 'Responsabilità civile nel diritto comparato' in *Digesto delle discipline privatistiche – Sezione civile* (1998) 12 ff.

Navone G., 'L'illecita pubblicazione di un numero di telefono su Internet è, di per sé, un danno immateriale?' (2025) *Foro it*. IV, 102

Nazzaro A.C., 'L'utilizzo dei Big data e i problemi di tutela della persona' (2018) 4 *Rassegna di Diritto Civile* 1239–1260

Page J.A., 'American Tort Law and the Right to Privacy' in Brüggemeier G., Colombi Ciacchi A. and O'Callaghan P. (eds), *Personality Rights in European Tort Law* (Cambridge University Press 2010), 38 ff.

Palmieri A., 'Consumatori, tutela collettiva, arbitrato: di miti (americani) infranti e timidi risvegli (europei)' in D'Alessandro C.A. and Marchese C. (eds), *Ius dicere in a globalized world* (RomaTre-Press 2018) 637 ff.

Palmieri A. and Altamura F. (eds), *Class actions e meccanismi di tutela collettiva. Le prospettive di sviluppo e le sfide della dimensione digitale* (Giappichelli 2023)

Palmieri A. and Pardolesi R., 'Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)' (2023) IV *Foro Italiano* 268 ff.

Pagliantini S., 'Un altro palcoscenico della "guerra" tra le corti: il danno (immateriale) bagatellare dell'art. 82 GDPR' (2023) IV *Foro Italiano* 268 ff.

Pardolesi P., *Arricchimento da fatto illecito: i rimedi. Dai disgorgement damages alla retroversione degli utili* (Cacucci 2023)

Pardolesi R. and Arcuri A., 'Analisi economica del diritto', in *Enciclopedia del diritto, Agg.*, VI (Giuffrè 2002) 7 ff.

Perlingieri P., 'L'informazione come bene giuridico' (1990) 2 *Rass. dir. civ.* 329 ff.

Pistor K., *The Code of Capital: How the Law Creates Wealth and Inequality* (Princeton University Press 201

Post R.C., 'Data Privacy and Dignitary Privacy: Google Spain, The Right to Be Forgotten, and The Construction of the Public Sphere' (2018) 67 *Duke Law Journal* 983 ff.

Pound R., 'The Economic Interpretation of the Law of Torts' (1940) 53(3) *Harvard Law Review* 365 ff.7

Procida Mirabelli di Lauro A., *La responsabilità civile. Strutture e funzioni* (Giappichelli 2004)

Procida Mirabelli di Lauro A., 'L'obbligazione come rapporto complesso' (2018) *Rivista di diritto civile* 917

Prosser W.L., 'Privacy' (1960) 48 *California Law Review,* 383 ff.

Renko J. 'Personal Data as Means of Payment for Digital Content or Digital Services in the Slovenian Implementation of the Digital Content and Services Directive' (2024) 74(5-6) *Zbornik Pravnog fakulteta u Zagrebu* 921

Resta G., 'The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives' (2011) 26 *Tul. Eur. and Civil Law Forum* 33 ff.

Resta G., 'Pubblico, privato, collettivo nel sistema europeo di governo dei dati' in Resta G. and Zeno-Zencovich V. (eds), *Governance of/through Big Data*, vol II (RomaTre-Press, 2023) 606 ff.

Ripstein A., 'Theories of the Common Law of Torts' in *Stanford Encyclopedia of Philosophy* (2022) https://plato.stanford.edu/entries/tort-theories/

Rotman L.I., 'Fiduciary Law's 'Holy Grail': Reconciling Theory and Practice in Fiduciary Jurisprudence' (2011) 91 *Boston Univ. Law Rev* 921-936

Rotman L.I., 'Understanding Fiduciary Duties and Relationship Fiduciarity' (2017) 62 *McGill Law Journal* 977

Ruda-González A., 'Liability for the unauthorised use of personal data in social networks: the case for collective redress' (2020) *European Journal of Privacy Law & Technologies - Special Issue* 80, 83

Salanitro U., 'Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia' (2023) 3 *Rivista di diritto civile* 426 ff.

Scognamiglio C., 'Danno e risarcimento nel sistema del RGPD: un primo nucleo di disciplina eurounitaria della responsabilità civile?' (2023) 5 *Nuova giurisprudenza civile commentata* 1150 ff.

Schwartz P.M., 'Preemption and Privacy' (2009) 118 *Yale Law Journal* 902 ff.

Scholz L., 'Private Rights of Action in Privacy Law' (2022) 63 *William & Mary Law Review* 1639 ff.

Sica S. and D'Antonio V., 'La commodification dei dati personali nella data driven society' in P Stanzione (ed), *I poteri privati delle piattaforme e le nuove frontiere della privacy* (Giappichelli 2022) 129 ff

Sica S., D'Antonio V., Giannone Codiglione G. and Sciancalepore G., 'Privacy, tutela del consumatore e risk based approach' *Comparazione e diritto civile* 1-21

Solove D.J., 'Lawsuits for HIPAA Violations and Beyond: A Journey Down the Rabbit Hole' (2014) *TeachPrivacy* available at: https://teachprivacy.com/lawsuits-hipaa-violations-beyond-journey-rabbit-hole/

Solove D.J. and Citron D.K., 'Standing and Privacy Harms: A Critique of TransUnion v. Ramirez' (2021) 101 *Boston University Law Review,* 62 ff.

Smith L., *The Law of Loyalty* (Oxford 2023)

Tilley C.C., 'Just Strict Liability' (2022) 43 *Cardozo Law Review* 2317 ff.

Trimarchi P, 'Sul significato economico dei criteri di responsabilità contrattuale' (1970) *Riv. trim. dir. proc. civ.* 512 ff.

Trocker N., 'La class action negli Stati Uniti: lo stato dell'arte' (2020) 2 *Rivista di Diritto Processuale* 754 ff.

Villanacci G., 'Autonomia privata e buona fede nella complessa relazione evolutiva con la normativa consumeristica' (2013) 4 *Contratto e impresa* 917 ff.

Waldman A.E., *Industry Unbound: The Inside History of Privacy, Data, and Corporate Power* (Cambridge University Press 2021)

Wendel W.B., 'Fiduciary Law' in Gold A.S., Goldberg J.C.P., Kelly D.B, Sherwin E. and Smith H.E. (eds), *The Oxford Handbook of the New Private Law* (Oxford University Press 2020) 312-323

Zaccaria A., 'La resistibile ascesa del contatto sociale' (2013) *Rivista di diritto civile*.77 ff.

Zetzsche D., Buckley R. and Arner D., 'The rise of TechFins: regulatory challenges' in J Madir (ed)*, FinTech. Law and Regulation*, 3rd ed. (Edward Elgar 2024), 415

Zoppini A., *Il diritto privato e i suoi confini* (Il Mulino 2020)


09:22 | Siena-Tirana Comparative Law Day
Scrivi qui il testo da cercare
D. HOXHA


K. KATRO


11:39 | Siena-Tirana Comparative Law Day


A. MANDILAKU
P. BROKA
C. NALDINI

CIP Katalogimi në botim BK Tiranë

Universiteti i Tiranës. Fakulteti i Drejtësisë
Siena-Tirana comparative law day : legal issues in the digital age : STCLD 2025 : proceedings book / University of Tirana, Faculty of Law, Department of Civil Law University of Siena, Department of Law. - Vlorë : Triptik, 2025.
372 f. ; 23 cm.

ISBN 9789928826800

1.Të drejtat civile 2.Baza të të dhënave 3.Mbrojtja 4.Konferenca
347 (062)
004.3 (062)

INTERNATIONAL SCIENTIFIC CONFERENCE

Siena-Tirana Comparative Law Day

LEGAL ISSUES IN THE DIGITAL AGE

STCLD 2025

PROCEEDINGS BOOK