Privacy Legal Relationships

Elena Sebiakina

Résumé

Ce travail vise à lancer une discussion sur la théorie générale du droit de la protection de la vie privée. L'auteur propose de commencer par une classification des relations juridiques dans le domaine de la vie privée, comme première étape vers l'identification des failles dans l'élaboration des règles de protection de la vie privée et l'application de la loi. La théorie relationnelle du droit, qui sous-tend ce travail, explique pourquoi chaque relation juridique en matière de protection de la vie privée prend sa propre direction et forme un objet d'une manière unique. La méthode utilisée dans ce travail est la classification des relations juridiques à l'aide des bases adoptées dans la théorie du droit civil. L'ouvrage identifie au moins dix types de relations juridiques en matière de protection de la vie privée, les interprète, les présente comme un système dynamique corrélé, met en évidence les modèles de leur existence et établit des parallèles entre certaines institutions du droit civil et le droit de la protection de la vie privée. En outre, le concept de relations juridiques permet de découvrir de nombreux mystères de la théorie du droit de la vie privée et nous apprend quel est l'objet du droit subjectif à la vie privée, quelles sont les obligations subjectives du responsable du traitement des données et où elles sont formalisées, pourquoi la notification de la vie privée est vitale pour un traitement licite, quelle est la nature juridique du consentement et de la notification de la vie privée, pourquoi le consentement recueilli « juste au cas où » ruine la stabilité des relations juridiques et bien d'autres choses encore.

Mots-clés : droit de la vie privée, classification, relations en matière de protection de la vie privée, taxonomie des relations juridiques en matière de protection de la vie privée

Abstract

This work is aimed at initiating of discussion on general theory of privacy law. The author suggests beginning with classification of legal relationships arising in privacy sphere, as a first step toward identifying the flaws in privacy rulemaking and law application. The relational theory of law, underlying this work, explains why each privacy legal relationship will take its own direction and will form an object in a unique way. The method used in this work is classification of legal relationships using the bases adopted from theory of civil law. The work identifies at least ten types of privacy legal relationships, interpret them, shows them as a correlated dynamic system, highlights the patterns of their existence and draws parallels between some institutions of civil law and privacy law. Also, the concept of legal relationships discovers many mysteries of theory of privacy law and teaches us what is the object of subjective privacy right, what subjective obligations actually has the data controller and where they are formalized, why privacy notice is vital for lawful processing, what is the legal nature of consent and privacy notice, why consent collected “just in case” ruins the stability of legal relationships and also much more.

Keywords: privacy law, classification, privacy relationships, taxonomy of privacy legal relationships

TABLE DES MATIÈRES

Introduction

In modern legal literature it is widely accepted that privacy is a complex category that encompasses various subjective rights and concepts.

The author aims to explore the reasons for this diversity by applying the concept of legal relationships. To the author's knowledge, no previous studies have examined privacy from such perspective or classified privacy legal relationships based on known criteria. This may be due to the uncertainty surrounding whether privacy law falls under private or public law, and whether the concepts or research methods of private law can be applied to privacy law as well. In this article, the author will investigate whether the privacy law belongs to private or public law.

The lack of certainty on privacy also leads different scholars and privacy experts to controversial legal qualifications of privacy as: property right[1], intellectual property right[2], intangible good[3], civil right[4], etc. In addition, considering privacy regardless of concept of legal relationships leads to rejection of the good sense ideas and assumptions inspired by similarities of privacy law with civil law (e.g., similarity of consent with an accept[5]).

The category of legal relationship is a scientific abstraction and a tool for legal research, commonly used within civil doctrine. Several authors in recent years have stressed, in various traditions, the need to take this tool into account and not only legal institutions or norms. This is a relational theory of law[6]. Agreeing with this approach, the author will place the concept of legal relationships at the center of its further reasoning on theory of privacy law.

The privacy sphere is a patchwork of many different legal relationships existing simultaneously among data subjects, data controllers, data processors, supervisory authorities, and other participants. This work is aimed to classify and typologize those myriads using the concept of legal relationship. Examination of legal phenomenon through legal relationship has a great advantage over normative and institutional analysis, because it allows a better visualization of the real situation in the light of legal facts, allows to see all elements functioning as a system, evaluate the connections between the parties, see the dynamic of relationships (towards or away, wider or narrower) and find the right solution or satisfaction.

The main approach in this work is an interdisciplinary approach, implying the enrichment of knowledge and methodology of general theory of privacy law at the expense of the methodology of theory of civil law. The main method of scientific research that author borrows from the theory of

---

[1] Lawrence Lessing, *Privacy as Property,* 69/1 SOCIAL RESEARCH 247ff (2002); Sevion DaCosta, *Privacy-as-Property: A New Fundamental Approach to The Right to Privacy and The Impact This Will Have on the Law and Corporation*, CMC SENIOR THESES 2635 (2021); Federal Trade Commission, *Competition and Consumer Protection in the 21st Century* (Sep 21, 2018), https://www.ftc.gov/system/files/documents/public_events/1408208/ftc_hearings_session_2_transcript_9-21-18.pdf at 108.

[2] Pamela Samuelson, *Privacy As Intellectual Property?,* 52/5 STANFORD LAW REVIEW 1125–73 (2000); Florian Faust, *Dateneigentum und Datenhandel,* in DATEN DEBATTEN, Band 3 (Hannes Bauer eds., 2019) 85ff.

[3] Adam D. Moore, *Intangible Property: Privacy, Power, and Information Control*, 35/4 AMERICAN PHILOSOPHICAL QUARTERLY 365ff (1998).

[4] Tiffany Li, *Privacy As/And Civil Rights*, 36/2 BERKELEY TECHNOLOGY LAW JOURNAL (2021).

[5]Maximilian Heller, *Rechtliche Einordnung der datenschutzrechtlichen Einwilligung* (2019), https://de.linkedin.com/pulse/rechtliche-einordnung-der-datenschutzrechtlichen-maximilian-heller.

[6] LUÍS ALBERTO CARVALHO FERNANDES, TEORIA GERAL DO DIREITO CIVIL: INTRODUÇÃO, PRESSUPOSTOS DA RELAÇÃO JURÍDICA (2012).

civil law is the method of classification, that is, the ordering of a multitude of phenomena and processes by dividing them into stable types. Any degree of classification represents a more advanced stage after collecting a body of disparate knowledge. Using the achievements of the theory of civil law in the classification of legal relationships as a blueprint, the author will apply some relevant bases of classification to privacy legal relationships and dividing them into stable types, give them its interpretation, see them as a system, highlight the patterns in their existence and draw parallels between some institutions of civil law and privacy law.

It will also help to build a logical taxonomy of legal relationships in the field of informational privacy and will support in the future, when new legal relationships arise, to classify them correctly and to attribute them to the correct type of legal relationships, to immediately understand the characteristics and patterns for this type. This is the key to understanding the origins of privacy multidimensionality.

Considering privacy as a dynamic system of legal relationships the author will try to answer many practical and theoretical questions, arising in the professional privacy communities, in particular: why the data subject has no right to demand the processing of its data? (see answer to question #1 in para F.I.); is the data subject obliged to provide true personal data to the data controller? (see answer to question #2 in para F.I.); why can't the data controller unilaterally "cancel" the data subject's consent? (see answer to question #3 in para F.I.); can the data controller be liable for violation of its own privacy policy on the website? (see answer to question #4 in para F.I.); what is the legal nature of the privacy notice? (see answer to question #5 in para F.I.); what is the legal nature of consent to data processing? (see answer to question #6 in para F.I.); is the privacy law private or public? (see answer to question #7 in para F.I.a.); why is the employer not always liable for its data leaks? (see answer to question #8 in para F.II.); why data processing based on consent, can't be terminated by termination of the contract with data subject? (see answer to question #9 in para F.II.); 10) why consent obtained "just in case" is wrong? (see answer to question #10 in para F.II.).

The answers to each question will be marked in the text (*in italic*).

A. Privacy theories and concepts

What we understand under informational privacy, is it a constitutional or civil right and what is its object?

It appears that the processing of personal data existed long before the terms were coined and before the first laws on the matter were enacted. From the beginning of speech, first personal data e.g., names, shoe and clothing size, pregnancy status, health condition, efficiency in hunting and battles — have been processed among tribesmen and elders for communications, marriage, purchasing, sewing, elections and other social contacts.

The Roman law can be somehow measured as a starting point to consider privacy as a legal value[7]. The "roman law of privacy" recognized and protected a bodily integrity, physical security, privacy of correspondence, privacy of religion right to honor and dignity[8].

In the Middle Ages, privacy was recognized through the right to private residence and the right to honor[9], which was reserved to a small segment of society and was not attributable to every person.

From a natural law perspective, the right to privacy could be counted with property and others among the rights pre-existing law.

Privacy is an excellent illustration of the circulation of concepts between common law countries and civil law countries, with mimicry phenomena that do not imply the disappearance of national traditions[10]. The notion of privacy has circulated well among laws, especially between the United States and Europe, even before its consecration in American constitutional law by the Supreme Court. It must be noted, however, that the integration of privacy into a large number of national and international laws is largely a matter of mimicry and knowledge of comparative law. The phenomenon of borrowing a term or concept is well known there. From the point of view of the study of law, the rise of privacy seems to be the result of the use of concepts in different legal systems regardless of their specificity (functionalism in comparative law).

The further evolution of humanity, the enlightenment and humanization of society, recognition of fundamental human rights along with the waves of industrial, technological and data revolutions, have led to the branching of privacy. As a result, new aspects of personal life are being recognized as people would like to control and protect from any uninvited interference.

With every new technology and new data processing method, with every new individual's self-extension[11] — it is likely that new rights will emerge in privacy. To date, at least following aspects of personal life deserve protection in democratic societies: personal and family life, communications, appearance, personality, identity, work, play, behavior, movement, location, housing, possessions, honor and dignity, professional and other secrecy, personal data, bodily parameters, digital persona, virtual person, geminoid.

The researchers distinguished seven different types of privacy based on correlation between spheres of personal life and technologies interfering them actually or potentially: privacy of the person, privacy of behavior and action, privacy of personal communication, privacy of data and

---

[7] Bernardo Periñán, *The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law*, 52/2 AMERICAN JOURNAL OF LEGAL HISTORY 183 (2012).

[8] *See* 1b. in the Table VIII "Torts or Delicts" of the Laws of the Twelve Tables (449 BC): "…If anyone sings or composes an incantation that can cause dishonor or disgrace to another… he shall suffer a capital penalty."

[9] *See* Periñán, *supra* note 7, at 198.

[10] Jean-Louis Halpérin, *L'essor de la «privacy» et l'usage des concepts juridiques*, 61/3 DROIT ET SOCIÉTÉ 765 (2005).

[11] JAMES WILLIAM, *THE PRINCIPLES OF PSYCHOLOGY* 291 (1890).

image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy) [12].

This work will focus on the study of informational privacy (privacy of data and image) in order to narrow the scope of this research.

The researchers Pamela J. Wisniewski and Xinru Page also compiled the most prominent privacy theories and frameworks from academic literature into the list[13]: privacy as information disclosure; privacy as interpersonal boundary regulation; privacy as contextual norms; privacy as affordances and design; user-centered privacy and individual differences.

Daniel Solove in his book Understanding Privacy[14] identifies six theoretical approaches to privacy commonly used in privacy analysis: 1) the right to be let alone — Samuel Warren and Louis Brandeis' famous formulation of the right to privacy; 2) limited access to the self — the ability to shield oneself from unwanted access by others; 3) secrecy — the concealment of certain matters from others; 4) control over personal information — the ability to exercise control over information about oneself; 5) personhood — the protection of one's personality, individuality, and dignity; and 6) intimacy — control over, or limited access to, one's intimate relationships or aspects of life.

“Privacy is not one thing, but a cluster of many distinct yet related things”, Solove wrote. As an umbrella term that brings together a group of concepts.

On the contrary, in Germany, the privacy right and the data protection right fall under such an umbrella construction as informational self-determination[15] (“informationelle Selbstbestimmung”), enshrined in the constitution and absorbing freedom of speech, right to active private life, right to education and the right to public sector information. Informational self-determination means the authority of the individual to decide itself when and within what limits information about its private life should be communicated to others[16].

In fact, the majority of listed above privacy concepts are relevant and true, all ideas are fair, because there are about a dozen different legal relationships, to which these concepts could be applied respectively. This is not an internal contradiction of privacy or a consequence of its complexity and subjectivity. The relational theory of law explains a lot about privacy: in each legal relationship privacy takes different direction and form an object of particular relationship in a unique way.

By subjective right to informational privacy here the author means the right of individual to independently establish a comfortable mode of access to and processing of information about it and its activities. Thus, the object of the subjective right to informational privacy will be the **degree of**

---

12 Michael Friedewald, Rachel Finn, David Wright, *Seven Types of Privacy* in EUROPEAN DATA PROTECTION: COMING OF AGE 3 (Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet eds, 2013).

13 Pamela J. Wisniewski, Page Xinru, *Privacy theories and frameworks* in MODERN SOCIO-TECHNICAL PERSPECTIVES ON PRIVACY 15 (Bart P. Knijnenburg, Xinru Page eds, 2022).

14 DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

15 German Federal Constitutional Court’s Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83.

16 Antoinette Rouvroy, Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* in REINVENTING DATA PROTECTION? (Serge Gutwirth, Yves Poullet eds, 2009).

confidentiality of information about data subject and its activities, established and maintained by the subject of this right.

B. Privacy law: from narcissism to altruism

Privacy and data-governance law have traditionally governed forms of private interpersonal exchange in order to secure the benefits of data-subject dignity or autonomy[17]. The focus on individual selfhood is expressed in the canonical concept mentioned above: informational self-determination. Many early and recent privacy concepts adopted the view of privacy as a control or an access with the data subject and its rights in the center. Privacy law's individualism is focused on foresight and protection of individuals from different forms of individual harm, ignoring the potential benefits and harm for whole social groups, which may entail inequality and discrimination. We could call this approach a "super-individual". It appears outdated in today's data-driven economy, where personal data serves as fuel.

Information and communication technologies treat most people not as individuals but as members of specific groups (or cohorts, classes, collections, crowds, populations and their segments etc.), where the groups are the really interesting focus, as carriers of rights, values, and potential risks. Especially big data is more likely to treat types (of customers, […]) rather than tokens (you, […]) and hence groups rather than individuals[18]. Targeting has been defined as "the act of directing or *aiming something at a particular group of people*" and "the act of attempting to appeal to a person or group or to influence them in some way"[19]. The EDPB notes in its Guidelines 2/2019, that tracking and profiling of users may be carried out *for the purpose of identifying groups of individuals with similar characteristics, to enable targeting advertising to similar audiences*. Such processing cannot be carried out on the basis of Article 6(1)(b), as it cannot be said to be objectively necessary for the performance of the contract with the user *to track and compare users' characteristics and behavior for purposes which relate to advertising to other individuals*[20].

The peculiar nature of the groups generated by big data analytics requires an approach that cannot be exclusively based on individual rights. The new scale of data collection entails the recognition of a new type of privacy, represented by groups' need for the safeguard of their collective privacy and data protection rights. This dimension requires a specific regulatory framework, which should be mainly focused on the legal representation of these collective interests, on the provision of a mandatory multiple-impact assessment of the use of big data analytics and on the role played by supervisory authorities[21].

---

[17] Salome Viljoen, *A Relational Theory of Data Governance*, 131/2 YALE LAW JOURNAL (2021) https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance at 370.

[18] Luciano Floridi, *Group Privacy – A Defense and an Interpretation* 18 (2017).

[19] See the definition of targeting in the Collins English Dictionary https://www.collinsdictionary.com/dictionary/english/targeting.

[20] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, para 56.

[21] Alessandro Mantelero, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in GROUP PRIVACY (Linnet Taylor, Luciano Floridi and Bart van der Sloot eds, 2017).

It seems unnatural today to consider privacy as a concept of individualism and alienation, as there is probably not a single person who would never have relations with other actors in the privacy sphere. For example, the research "Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users"[22] shows, that self-disclosure decisions goes far beyond self-disclosure and may also include confidant disclosures (co-owned information shared by others), relationship boundaries disclosures (e.g., deciding with whom to connect), network boundaries disclosures (e.g., giving others access to one's connections) and territorial boundaries disclosures (e.g., managing content and interactions across public, semipublic, and private spaces). Taking this more interpersonal perspective to modern privacy acknowledges that people are inherently social, and privacy must be considered in relation to sociality rather than to isolation[23].

Privacy arises always in relationships between an individual and someone present or someone potential (expectation of observation) or someone existed in the past. Even if the last human on Earth (a situation of seemingly absolute personal freedom), privacy is likely to remain as a thought and expectation of future observator who may come, see, and judge a human's home, belongings, creations, or writings. For someone it could be the feeling of God, as an outside observer. In any case, even the last human on Earth will always behave in accordance with the feeling or premonition of an extraneous look, and its freedom will always be limited by it.

This idea brings us closer to the concept of legal relationship: unlike the social relation, which objectively exists and manifests itself in the specific actions of the participants, the legal relationship is only conceived, exists ideally, regardless of whether its participants know about it or not. Legal relationships are often not realized by its participants, they may not be aware of their participation in some legal relationship, but nevertheless they will remain its subjects endowed with subjective rights or legal obligations.

In recent years, there has been a growing trend in theory of privacy towards relational conceptualizing it as a matter of relationships (social relationship[24], contextual integrity[25], data relations[26] or relationship of trust[27]) or as a collective interest (associational privacy[28], group

---

[22] Pamela Wisniewski, Najmul Islam, Heather Lipford and David Wilson*, Framing and Measuring Multidimensional Interpersonal Privacy Preferences of Social Networking Site Users,* 38 COMMUNICATIONS OF THE ASSOCIATION FOR INFORMATION SYSTEMS 239 (2016).

[23] *See* Wisniewski et al., *supra* note 13, at 23.

[24] James Rachels, *Why privacy is important* in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand David Schoeman ed, 290, 294 (1984).

[25] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

[26] *See* Viljoen, *supra* note 17, at 603.

[27] Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 UNIVERSITY OF MIAMI LAW REVIEW 559 (2015).

[28] Laura K. Donohue, *Correlation and Constitutional Rights*, forthcoming in WITHOUT TRIMMINGS: THE LEGAL, MORAL, AND POLITICAL PHILOSOPHY OF MATTHEW KRAMER (Mark McBride, Visa A.J. Kurki, 2020) http://dx.doi.org/10.2139/ssrn.3678024.

privacy[29], relational privacy[30], privacy externalities[31], public good[32] or privacy dependencies[33]). For example, Salome Viljoen developed her relational theory of data governance and identified two types of data relations: vertical and horizontal[34].

Finally, the theory of privacy law refocuses on more than one individual. After all, an individualistic model fails to protect data subjects whose privacy depends on others but whose consent will never be asked. We are talking about privacy of groups, which could be either: knowingly created by data subjects[35] (e.g. spouses, relatives, friends, classmates, fellows, colleagues, companions, visitors of an event, marathon runners, etc.) or generated by data controllers without data subjects knowing[36] (e.g. types, cohorts, users, classes, populations, segments, etc.).

Step by step, privacy law moves to recognition of the collective interest as a subjective good to be protected, and of different types of groups as parties of legal relationships in privacy sphere. In the context of this work, by groups we mean the multiplicity of persons on one side of the legal relationship — where there was usually only one data subject, there now could be a group united by one characteristic or feature, one protected or violated interest. And this, conditionally speaking, "legal capacity" of a group of data subjects is no longer limited to participation in trial, e.g., class actions (US, UK) or collective consumers' actions (Europe)[37].

---

[29] *See, e.g.,* Edward J. Bloustein, *Group privacy: the right to huddle*, 8 RUTGERS-CAMDEN L.J. 219 (1977); LINNET TAYLOR, LUCIANO FLORIDI AND BART VAN DER SLOOT, GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (2017); Anton Vedder, *KDD: the challenge to individualism,* 1 ETHICS AND INFORMATION TECHNOLOGY 275ff (1999); *See* Floridi *supra* note 18; Michele Loi, Markus Christen, *Two Concepts of Group Privacy,* 33 PHILOS. TECHNOL. 207ff (2020).

[30] Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249 (2012).

[31] Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J. L. & POL'Y FOR INFO. SOC'Y 425 (2011).

[32] Joshua A.T. Fairfield, Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 452 (2015).

[33] Solon Barocas, Karen Levy, *Privacy Dependencies,* 95 Washington Law Review 555 (2020).

[34] The vertical relation is between data subjects and data controllers and involves the exchange of personal data for digital services. It is expressed technically through data flow and legally through contractual terms and consumer-privacy laws. The horizontal relations, on the other hand, describes how data production connects data subjects to others who share similar characteristics. This is expressed through informational infrastructures that group people based on shared preferences, social patterns, and behaviors. These relations are population-based rather than one-to-one and link individuals together via webs of horizontal connection.

[35] The revealing by one member of data related to every other member will affect the privacy of the whole group, although the other members will not have the opportunity to object or protect their interests. They won't be asked.

[36] Some manipulative targeting techniques can negatively affect entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups (*see* 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 (Digital Services Act), recital 69).

[37] *See* Pulina Whitaker, Chris Warren-Smith, Alexandre Bailly, Ezra D. Church, *Insight, US, UK and EU collective actions in the privacy and cybersecurity space* (2023), https://www.grip.globalrelay.com/us-uk-and-eu-collective-actions-in-the-privacy-and-cybersecurity-space.

Such concepts as social, socioeconomic, and environmental benefits[38], benefits of local communities, collective interests of consumers[39], collective interests of recipients of the service[40], harm to collective interests of consumers[41], harm to collective interests of individuals[42], data cooperatives, data altruism — now sound not only from researchers' and scientists' horns[43], but also occupy places in the legislation.

For example, Data Governance Act[44] introduces the concept of data cooperative — an organization constituted by data subjects (or one-person undertakings or SMEs), which represents the group and supports with execution of privacy rights, negotiates terms and conditions of data processing in favor of the group or seeks the solutions to potential conflicts of interests when data relates to several data subjects within that group. The Data Governance Act enables also collective complaints and lawsuits in Article 27.

The Artificial Intelligence Act considers the group of natural persons as an independent subject of right violations or harm, for example, according to Recital 31 "AI systems providing social scoring of natural persons by public or private actors may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice [*author's comment: of certain groups*]. The social score obtained from such AI systems may lead to the detrimental or unfavorable treatment of natural persons or whole groups thereof in social contexts..."

Article 80 of General Data Protection Regulation (GDPR) not only enables data subjects, where provided for by Member State law, to mandate a group representative: not-for-profit body, organization or association, – for protection their data, lodging complaints, exercising the privacy rights and receiving a compensation, but also enables such representatives to act independently of a data subject's mandate, to lodge a complaint with the supervisory authority and to exercise privacy rights if it considers that the rights of a data subject under GDPR have been infringed as a result of the processing.

---

[38] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, art 14 (2a).

[39] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, art 1; See also Digital Services Act, recital 119.

[40] Digital Services Act, recitals 124, 128, 138.

[41] 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 (Digital Markets Act), art 42 and recital 104.

[42] *See* EU Artificial Intelligence Act, art 3 para 1 points 44 e and 44 f. The legislator here even measures the "collectivity" of interests of individuals with the number of affected Member States (*widespread infringement*) or in proportion of population of the Union (*widespread infringement with a Union dimension*).

[43] *See* in Thomas Hardjono, Alex Pentland, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management* (2019): "The … collective organization is required to move from an individualized asset-based understanding of data control to a collective system based on rights and accountability, with legal standards upheld by a new class of representatives who act as fiduciaries for their members." https://www.researchgate.net/publication/333309091_Data_Cooperatives_Towards_a_Foundation_for_Decentralized_Personal_Data_Management/citation/download; Miller Katharine, *Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data*, STANFORD HAI (2021), https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data.

[44] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

As Luciano Floridi predicted in 2017, "by grouping people according to specific criteria we create an individual (the group), which can both be targeted and claim to have rights as a group"[45]. Recognition of legal personhood of groups and collectives by laws is a big step towards legislative recognition of groups as participants of legal relationships in informational privacy sphere (further — ***privacy legal relationships***).

Also, the Finnish Secondary Use Act 2019[46] focuses on data about groups of people instead of individuals. It also refers to such social benefits from processing of "group data" as: better and more effective care and treatment than before, minimization of wellbeing and health differences, development of new health technologies and applications, etc. At the endpoint these group benefits must lead to individual benefits for each citizen: more personalized health services instead of basic health services only or costly chronic disease management.

And it can be called a catharsis of privacy concept's development — the movement towards its opposite — data altruism, when personal data is voluntarily made available by individuals or companies for common goods as better healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest (see Article 2 (10) of DGA).

Thus, not only individuals may enter privacy legal relationships with other data subjects, data controllers and other participants of data processing, but also groups of data subjects may knowingly or not be parties to privacy legal relationships. Some types of groups may generate among their members also internal legal relationships, mainly organizational or data processing.

C. Legal relationships as a jural fiction: back to basics

It can be assumed that one of potential reasons why views on privacy are so polyphonic, could be disregarding the fact that actors in privacy sphere participate in many completely different legal relationships, sometimes simultaneously. And they could be not only public but also private. The object of such relationships could be different: the personal non-property good or personal data itself or its processing.

It is impossible to consider privacy in general, as a coherent phenomenon and assess it without taking into account the key element to study – legal relationships. This approach is tantamount to trying to consider in general all civil or all constitutional law, without distinguishing separate categories and institutions. That would be a mistake.

As in any branch of jurisprudence, the most important and central element of study is the connection arising between actors – a legally regulated interconnection between its participants.

---

[45] *See* Floridi, *supra* note 18, at 10.

[46] *See* GDPR Brief: the Finnish Secondary Use Act 2019 (21 May 2020), https://www.ga4gh.org/news_item/ga4gh-gdpr-brief-the-finnish-secondary-use-act-2019-may-2020-bonus-brief.

The legal relationship is one of the fundamental concepts of law, following the subjective right. It serves as a systemic starting point for the study of law, as it encompasses all rights or powers, corresponding duties or obligations, subjects and objects[47].

In the 19th century, the influential pandectist and legal theorist Friedrich Carl von Savigny determined the legal relationship as a relation between person and person, determined by a legal rule[48].Using a systematic method of cognition, he places legal relationship (not a subjective right) at the basis of his system of studying roman law. In his opinion, existing within the system, all legal relationships form one organic whole, but we divide it into elements so that they consistently reach our consciousness and could be transmitted to others[49]. Savigny distinguished such elements of legal relationship as subjects, objects[50] and subjective rights.

Continuing the systematic approach to analysis of law, Hohfeld proposed eight conceptions inside legal relationships: right/duty, privilege/no-right, power/liability and immunity/disability[51]. He also determined the right to privacy as a claim-right, not relating directly to either a person or a tangible object[52].

Nowadays Simon Fisher also sees the roots of legal relationships' concept in Roman law, where persons, things (property and obligations) and persons' interactions about things form 3 elements of legal relationships[53]. In jurisprudence the abstract definition of a legal relationship is referred to as "jural relation". Although Roman law did not have a term for jural relations, a number of German writers in the 1860s included the concept in legal treatises[54]. The Italian interpretation of the term "legal relationship" in civil law system is a "rapporto giuridico" defined as "every interpersonal relationship regulated by law"[55].

An American professor of law Albert Kocourek defined "legal relations" as actual or assumed relationships, and "jural relations" as the abstraction of the juristic elements of a legal relation[56]. And German professor Norbert Achterberg defined legal relationship as social relationship regulated by means of the law[57].

---

47 JÖRG NEUNER, ALLGEMEINER TEIL DES BÜRGERLICHEN RECHTS (GROßES LEHRBUCH) 221 (2023).

48 FRIEDRICH CARL VON SAVIGNY, SYSTEM DES HEUTIGEN RÖMISCHEN RECHTS. BAND 1, para. 52, 333 (1840).

49 *Id.* at 267.

50 *Id.* at 486.

51 Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning,* YALE UNIVERSITY PRESS 710 (19I7).

52 *Id.* at 734.

53 Simon Fisher, *The Archival Enterprise, Public Archival Institutions and the Impact of Private Law*, vol. 26/2 ARCHIVES AND MANUSCRIPTS 335 (1998).

54 LIVIA IACOVINO, RECORDKEEPING, ETHICS AND LAW: REGULATORY MODELS, PARTICIPANT RELATIONSHIPS AND RIGHTS AND RESPONSIBILITIES IN THE ONLINE WORLD 78 (2006).

55 GIUSEPPE LEROY CERTOMA, THE ITALIAN LEGAL SYSTEM 19ff (1985).

56 ALBERT KOCOUREK, JURAL RELATIONS 31 and 75ff (1928).

57 NORBERT ACHTERBERG, DIE RECHTSORDNUNG ALS RECHTSVERHÄLTNISORDNUNG. GRUNDLEGUNG DER RECHTSVERHÄLTNISTHEORIE 18 (1982).

It's important to note, that concept of legal relationship is not a private law concept only. For example, an American philosopher and professor Matthew Henry Kramer extends the Hohfeldian concept of legal relationships to public law[58]. Also, an English jurist William Blackstone presented constitutional law as such of public and private legal relationships between rulers and subjects. Further continental European legal thinking split the legal relationships in the state into individual relationships between state organs and with individuals[59]. Thus, regardless of whether we classify the privacy law as public or private law, using the concept of legal relations to study it is quite justified.

Despite the reception of the concept by the modern civil codes and its great spread, the concept of legal relationships was discredited as an approach to legal analysis[60]. Still, examination of legal phenomenon, through legal relationships has a great advantage over normative and institutional analysis, because it allows a better visualization of the situation in the light of legal facts, allows to see all elements functioning as a system, evaluate the connections between the parties, see the dynamics of relationships (towards or away, wider or narrower) and find the right solution or satisfaction.

Actually, the category of legal relationship serves as an ideal concept within civil doctrine. It is a scientific abstraction and a tool for legal research. Several authors in recent years have stressed, in various traditions, the need to take this tool into account and not only legal institutions or norms. This is a relational theory of law[61]. Agreeing with this approach, we will place the concept of legal relationships at the center of our further reasoning on theory of privacy law.

D. The structure of legal relationship

Before diving deeper into classification, I suggest stopping at one important aspect of legal relationship: its structure. My upcoming work will be devoted to its detailed consideration. For now, we will only touch at a high level on two approaches to the structure of legal relationships.

Classical doctrine distinguishes four elements – subject, object, subjective rights, and subjective obligations. But there are also various views, one of which belongs to Emmanuel Jeuland (relational theory), who counted 6 elements in the legal relationship[62].

Although the author will rely on the first 4-elements' structure in this work, the multi-elements' structure deserves mentioning here to sow the seed of conjecture: more likely the different concepts of privacy to some extent came close to the idea of legal relationships, groped and focused on only one of the elements, making it the center of each single concept (norms, context, trust, etc.) and leaving the rest of the elements of legal relationships unattended.

---

[58] *See* Donohue, *supra* note 28, at 2.

[59] *See* ACHTERBERG, *supra* note 57.

[60] Rodrigo Brum Sulva, *A importância do conceito de relação jurídica*, 2415 REVISTA JUS NAVIGANDI (2010).

[61] *See* FERNANDES, *supra* note 6.

[62] *See* EMMANUEL JEULAND, THEORIES OF LEGAL RELATIONS (2023).

E. The classification of privacy legal relationships

I. Absolute and relative

One of the most dogmatic classifications, not only due to the difficulties and doubts about it raised by the doctrine, but also due to the differences of regime that are linked to it, opposes absolute legal relationships to relative legal relationships[63].

Depending on the degree of certainty of the parties of legal relationship, the theory of law divides them into absolute and relative. In absolute legal relationships, only one subject is precisely defined on one side — the active person, who is opposed by an unlimited number of undefined passive persons on the other side. These legal relationships justify a right in relation to all others (*erga omnes*): we could say that its core is a freedom that the legal system guarantees to a person by excluding everyone else from it[64]. The latter then have the duty to respect this right and not to infringe it. It is what is called a general duty of respect or universal passive obligation. The absolute legal relationship exists latently between the active subject and all persons who are in conditions to violate the subjective right[65].

Thus, privacy relationships, regulated by the Universal Declaration of Human Rights, European Convention on Human Rights (further – ECHR), the International Covenant on Civil and Political Rights and many Constitutions, where the privacy right is declared and recognized for any person – should be classified as absolute legal relationships. All individuals must refrain from disclosing the personal data of data subject unless it has instructed otherwise. The circle of obliged persons is not delineated here, as the obligation not to violate the informational privacy of data subject lies with everyone, both natural and legal persons.

Absolute privacy legal relationships are characterized by the fact that all obligated persons must refrain from actions that violate the absolute right of data subject to independently establish the comfortable access mode to its personal data.

It is worth mentioning here, that the right to privacy is not an absolute right, but a qualified one[66]. This right not only clashes with freedom of expression and freedom of the press, but also, with the interests of national security, public safety or the economic well-being of the country, the necessity of prevention of disorder or crime, of protection of health or morals, or the necessity of protection of the rights and freedoms of others (as stipulated in Art. 8(2) ECHR). So, even though privacy right is a core of absolute privacy legal relationships, this right itself is not absolute.

A relative legal relationship is a legal connection whose parties are identified and ideally known to each other. For example, in the legal relationships regarding processing of personal data of users in a social network, a particular data subject is opposed by a concrete data controller on the other

---

63 *See* FERNANDES, *supra* note 6, at 118.

64 *See* NEUNER, *supra* note 47, at 223.

65 *See* FERNANDES, *supra* note 7, at 119.

66 *See* Periñán, *supra* note 7, at 188.

side – the owner of the social network and behind it the other processing participants: possible joint-controllers, processors, sub-processors, co-controllers, exporters, importers and other representatives (further – processing participants). Hereinafter, I suggest understanding a processing representative as a person who, by instruction of a processing participant, is obliged to process personal data (or participate in the processing) on its behalf and in accordance with its instructions.

An obligation arises between the parties of a relative legal relationship, where data controller is obliged to comply with the mandatory and declared characteristics of personal data processing established by law or voluntarily taken over (further — characteristics of data processing), and data subject has the right to claim its fulfillment from data controller.

As a result of defining the content of the relative legal relationship of data processing in this way, the data processing itself is neither the object of such a legal relationship nor the subjective obligation of data controller, and the subject does not have a subjective right to demand the processing of its personal data, except the processing while the execution of some rights to rectification, object and erasure *(Answer to question #1)*. Likewise, the data subject in these legal relationships has no subjective obligation to provide the data controller with its personal data or to provide them truthfully (except in cases when the obligation to provide it or its accuracy is directly stipulated by law or the controller's requirements), and the data controller has no corresponding right to demand it. For example, it is impossible to hold a job applicant responsible for false information about hobby in its resume, and creative professionals are entitled to use a pseudonym or change their appearance *(Answer to question #2)*. Meanwhile, according to rules of some online services, the accuracy of personal data may be an obligation of data subject, under penalty or ban. Whereas, even after obtaining the data subject's consent, the data controller is not obliged to start data processing. It is entitled to never start it *[Author's note: on which, in my opinion, data subject has right to be informed]*.

So, data subject has right to demand proper performance of data processing in accordance with declared characteristics (how data should be processed?), but it has no right to demand the processing itself (should data be processed or not?), including the dissemination or higher publicity of personal data when data subject needs it.

Only the data controller itself decides whether data processing will begin. At the same time, the controller is not entitled to unilaterally “revoke” the provided consent, due to the irrevocability of the consent's request *(Answer to question #3)*, which by its legal nature, as we will see below in the section on accessory legal relationships, is an analogue of the offer. Still data controller can refuse from any data processing at its own discretion, and it may also stop any existing data processing at any time, except in cases when such processing arises from legal obligations from which the controller cannot refuse, e.g., the obligation to provide medical care, contractual services, fee payments, etc.

Nevertheless, data subjects have subjective rights to terminate or modify relationships regarding the processing of their personal data, e.g., execute the right to be forgotten, to withdraw consent, to change personal data, and in some jurisdictions, suspend a specific type of processing or switch to another data controller.

Coming back to the controller's obligations to comply with the mandatory and declared characteristics of data processing: they may be contained not only in legislation or, for example, in the text of the consent's request (which is usually called simply “consent”), but also in other public or corporate documents of data controller, e.g., in: a) public assurances: published privacy policy or privacy declaration, privacy notice, terms of use[67], compliance marks, privacy code, industry code of conduct, to which the controller joined; b) corporate rules on: personal data protection, data subject requests' processing, response to data breach, work with personal devices, information security, storage and deletion, remote work, intra-group personal data exchange, job descriptions, employees' obligations, etc.

In author’s opinion, subjective obligations that the controller voluntarily undertook and brought to the subjects' attention to encourage them to enter legal relationships of the data processing, have the legal nature of civil obligations and are subject to administrative or civil liability.

Therefore, the data controller who provided the data subject with false assurances on the characteristics of data processing from the beginning of their relationships, misleading data subject by it, must bear at least civil liability, namely: the data controller must compensate the data subject for damages caused by the inaccuracy of such assurances or cease processing upon data subject's request *(Answer to question #4)*. Similarly, the invalidity of subsequent changes in the characteristics of data processing (e.g., false promises to implement end-to-end encryption[68]) must result in civil liability for violation of data controller's obligations.

Even if, before entering legal relationships of data processing, the data subject had no opportunity to familiarize themselves with all the characteristics of future data processing and all public assurances of data controller[69] to make an informed decision, it has the right to subsequently refuse data processing or demand its termination, blocking, or deletion of its personal data. The decision to remain in a relationship with the data controller or leave – will be, not least, based on the data controller's public assurances. And if it turns out that the data subject entered privacy legal relationships under the influence of deception or material error caused by inaccurate assurances, it should have the same protection as usually have any other participant of civil legal relationships.

Thus, in a relative privacy legal relationship, the parties have mutual rights and obligations, which means that data subject must know exactly the counterparty from which it can demand the fulfillment of obligations, and to whom it should claim the execution of its subjective rights.

---

67 “In particular, platforms use contracts systematically to facilitate and protect their own legibility function, extracting transparency from users but shielding basic operational knowledge from third-party vendors, users, and advertisers alike. The particular form of the access-for-data contract – a boilerplate terms-of-use agreement not open to negotiation – asserts a nonnegotiable authority over the conditions of access that operates in the background of even the most generative information-economy service. Boilerplate agreements are contractual in form but mandatory in operation, and so are a powerful tool both for private ordering of behavior and for private reordering of even the most bedrock legal rights and obligations. (JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM, 44 (2019); *See, e.g.,* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013)).

68 An example of a false promise of changes in processing that misled millions of users was the video conferencing provider Zoom, which began stating in their marketing materials that they used end-to-end encryption, which turned out to be transport encryption, providing less protection for personal data A class action lawsuit filed by data subjects against Zoom in California in 2022 resulted in a settlement of $85 000 000 to the data subjects, https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

69 According to research by Aleecia McDonald and Lorrie Cranor, if people were required to read all relevant privacy notices, it would take over 200 hours per year (Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 565 (2008)). Even if everyone suddenly started reading privacy notices, they often cannot understand the information they receive about their data and are not able to make informed decisions (Daniel J. Solove, *The Limitations of Privacy Rights*, NOTRE DAME LAW REVIEW 996 (2023)).

That is why the controller's obligation to inform data subject about the processing and its characteristics (if personal data was not obtained from data subject directly) must be crucial for any data protection legislation worldwide. Otherwise, data subject remains wandering in the dark — with whom it is in a legal relationship (if it is even aware of it), it is deprived of the ability to demand the fulfillment of obligations from data controller due to its unknown identity and loses the ability to execute the subjective rights. It is deprived of any information about the degree of confidentiality/accessibility of its personal data, and therefore, the ability to exercise the privacy rights.

This situation is very similar to such a privacy violation as exclusion[70] – leaving an individual unaware of data processing, which serves as a basis for forming biased opinions/conclusions about it or producing negative consequences that hinder its opportunities. The lack of privacy notice could also be classified as a "relationship harm"[71]: a damage to the trust that is essential for the privacy relationship, which is fiduciary[72].

From the civil law perspective, the notification of data subject about data processing could be qualified as a legal communication and a legal fact that generates a legal relationship of data processing (*Answer to question # 5*).

Therefore, until such notification is received by the data subject, the lawful processing of personal data apparently cannot occur and should be classified as an unlawful processing of personal data. In addition, failure to notify the data subject grossly violates its right to freedom of entry into legal relationships: the individual is involuntarily involved in illegal relationships, which restricts its legal capacity.

Not everyone understands why privacy notice is critically important for lawfulness of privacy legal relationships, and many practicians perceive it as some kind of annoying burden of data controller. Though privacy notice is about the data subject's awareness of its own participation in legal relationships and of the controller's specific obligations. It is crucial for exercising of legal capacity by any individual.

If the data subject does not know the data controller, does this mean that the latter de facto releases itself from all its obligations to the data subject? After all, no one can demand the fulfillment of obligations of which it is not aware.

It is also important to note that the absolute legal relationship arises between data subject and all capable data controllers without exception. And when data subject enters relative legal relationship, the counterparty is always a party of already existed absolute legal relationship. Just because there is no (or at least should not be) such a third party who would not be in an absolute privacy legal relationship with the data subject. So, this absolute legal relationship will remain, and will continue to exist between both parties in parallel with the new relative legal relationship.

---

[70] *See* Taxonomy of harm based on Daniel's Solove Taxonomy of Privacy by Enterprivacy Consulting Group, version 7 (2023), https://enterprivacy.com/tools-resources.

[71] Danielle Keats Citron and Daniel J. Solove, *Privacy Harms*, 102 Boston University Law Review 859 (2022).

[72] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, 103 (2004).

Further thinking on parallel existence of two legal relationships between same participants, leads us to the idea, that data controller's employees (and other representatives) also participate simultaneously in two legal relationships with data subject: directly in an absolute legal relationship and indirectly as a representative in relative legal relationships of data controller. That is why, in the event of a violation of data subject's privacy rights by an employee, the employer will not always be liable.

An employee is personally liable for violation of its own subjective obligations from absolute legal relationship with data subject, acting there as an independent party, but not a structural element of data controller. Acting under data controller's instructions, employee performs its representative role and therefore is not liable for the violations caused by employer's instructions *(Answer to question #6)*. Thus, in the case of investigation of data leak (or any other privacy violation), it is crucially to differentiate in what role and in which legal relationship the employee was at the moment of violation, in order to determine — which particular subjective obligation was violated: 1) own subjective obligation from an absolute legal relationship with data subject (passive obligation to comply with the access mode to personal data established and maintained by the data subject) or 2) data controller's subjective obligation from its relative legal relationship with this data subject (obligation to comply with characteristics of data processing). In the second case the data controller will more likely be liable for the employee's violation.

I.a. Qualification of specific data protection laws: private or public?

The above classification of privacy legal relationships brings us closer to answering this question.

The fragmentation of approaches and concepts of privacy is also facilitated by the fact that privacy in various forms is not only a fundamental constitutional human right enshrined in constitutions and international conventions, but also an intangible object of civil rights and a personal good enshrined in civil codes, e.g. article 9 of Civil code of France, § 823 II of German BGB, part 4 of China's Civil code, article 709 of Civil code of Japan, Articles 12, 20, 21 of Civil code of Brazil, etc.

For example, German civil law classifies the following incorporeal objects as objects of sovereign civil rights: name, picture, the content of a private letter, the handwriting, recorded voice, other manifestations of the personality[73]. And French civil law distinguishes among subjective civil rights such individual rights as right to physical integrity, right to moral integrity (respect for his

[73] *See* NEUNER, *supra* note 47, at 317.

honor, right on the image, respect of the privacy), right to name[74], etc. The lawyers also show parallels of some concepts and institutions of civil and privacy law[75].

This creates a dilemma of classifying specific privacy regulations as an extension of public or private law. More precisely, in relation to which generic laws will the existing privacy regulations be considered as specific — to constitutions (public law) or to civil codes (private law)?

First, constitutions and conventions declare subjective rights which are the objects of absolute legal relationships between data subject and all others. Whereas specific legislation, as GDPR, regulates principally relative privacy legal relationships, which arise between specific parties, and in cases when those parties are equal[76], such legal relationships should be considered as private. While if one of the parties exercises its authority, such legal relationship should be considered as public. Meanwhile, participation of public body in the legal relationship doesn't make it public as this is not the only feature. Two other signs of public legal relationships, in addition to participation of the bearer of state power are: 1) there should be a vertical of subordination between the parties, 2) the public body should perform its powers and act as prescribed by laws and administrative regulations, 3) the public body is not free in exercising its rights or fulfilling its obligations, because the state directly stands behind it as an invisible third party (or puppet master), whose rights, obligations and public interests are exercised by this public body.

Secondly, the public bodies, involved in the private relative legal relationships of data processing does not exercise their authority, rather act similarly to a regular data controller, performing subjective obligations established for them by specific privacy legislation, privacy policy, contracts, and internal rules. Public bodies under most democratic civil codes stand equal with other participants of civil legal relationship, with other participants of privacy legal relationship, which is a type of private legal relationships. [*Author's note: keep in mind that relative public privacy legal relationships will also be considered in chapters 5 and 6 below.*]

Thirdly, as discussed in the previous chapter, data controller with data subject simultaneously participates in two types of parallel legal relationships: absolute and relative. So, the controller may properly fulfill its obligations from both or may violate its obligations from one or both.

It would be logical to assume that in case of violation of obligations from absolute privacy legal relationship, the data controller should be liable under public (e.g., administrative or criminal) law and in case of violation of its obligations from relative privacy legal relationship, data controller

---

74 BRIGITTE HESS-FALLON, ANNE-MARIE SIMON, MARTHE VANBREMEERSCH, DROIT CIVIL 81 (2017).

75 *See e.g.,* Louisa Specht, *Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit* – Eckpfeiler eines neuen Datenschuldrechts, Rheinische Friedrich-Wilhelms-Universität Bonn DGRI-Jahrbuch (2017) https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Specht_Datenschuldrecht4.pdf; Louisa Specht, *Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels,* DGRI Jahrbuch 2012, edited by Matthias Scholz and Axel Funk, Köln: Verlag Dr. Otto Schmidt, 2014, pp. 239-248; Jim Harper, *Personal Information is Property* (2024) https://ssrn.com/abstract=4691923; Maximilian Heller, *Rechtliche Einordnung der datenschutzrechtlichen Einwilligung* (2019), https://de.linkedin.com/pulse/rechtliche-einordnung-der-datenschutzrechtlichen-maximilian-heller; Maximilian Heller, Daten als Zahlungsmittel (2019), https://www.linkedin.com/pulse/daten-als-zahlungsmittel-maximilian-heller; Hannes Bauer et al., *Dateneigentum und Datenhandel.* Berlin: Erich Schmidt Verlag (2019).

76 For example, according to Article 3 (15) and Recital 19 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC: the controller must seek a freely given consent even given the clear imbalance between the data subject and the controller (a public body). It means that legislator presumes that both parties of legal relationships stand equal, and that data subject has the right to refuse to enter these relationships even with a public body.

should be liable under private law (e.g., privacy regulations), even if the party of such relationship is a public body. [*Author's note: but violations of controller's obligations from relative public relationships will result in liability under public law.*]

In practice, the concept of administrative fines for privacy violations and other infringements of privacy regulations, provided for by specific data protection laws, is an element adopted from public administrative law, as is the procedure for their imposition by supervisory authorities. Whether in specific data protection laws or administrative codes, these norms of public law are still an integral part of private law. It is probably due to the legislator's intention to emphasize the degree of social danger of privacy violations, equating them with administrative offenses[77], and in some countries, with criminal offenses[78].

So, the answer to the above question: the specific data protection laws are private as the main legal relationships they are aimed to regulate are – private[79], but those laws may contain some elements and concepts of public law, as administrative liability or public legal relationships with supervisory authority, as a party.

Many branches of law are a mixture of different public and private elements. Public principles emerge from private branches of law (e.g., the relationships between subsidiary and a parent company, stock issue, reporting to the stock exchange, etc.). And private law principles are gaining their place in traditionally public branches, for example, procedural law (e.g., settlement agreement). Therefore, attempting to classify the privacy law solely as private or public is hardly productive (*Answer to question #7).*

II. Principal and Accessory

If we look at any list of legal bases for data processing as at the list of legal facts provoking the emergence of privacy legal relationships, it becomes clear that most of the latter arise as accompanying some kind of principal relationships: providing medical assistance to data subject, public services, participation in a research, performing of legal obligations by the data controller with respect to data subject — data processing will inevitably arise as an accessory, dependent, appurtenant, so we could qualify it as accessory legal relationship. It means that most privacy legal relationships are accessory or secondary in respect to the principal legal relationships which serve as catalysts for processing of personal data and privacy legal relationships.

---

[77] German Federal Data Protection Act of 30 June 2017, s 41 (1); GDPR, art 84; Argentina Personal Data Protection Law No. 25,326, art 31.

[78] German Federal Data Protection Act of 30 June 2017, s 41 (2); French Penal Code, articles 226-1—226-9; Privacy Act 1988 of Australia, art 3A; Privacy Act 1988 of Australia "offence against this Act", subsection 6; Argentina Personal Data Protection Law No. 25,326, art 32.

[79] GDPR, art 1(1): "this Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."; Personal Information Protection Law of the People's Republic of China, art 1: "This Law is enacted in accordance with the Constitution for the purposes of protecting the rights and interests on personal information, regulating personal information processing activities, and promoting reasonable use of personal information."; Indian Digital Personal Data Protection Act, 2023, art 3.a: "Subject to the provisions of this Act, it shall apply to the processing of digital personal data within the territory of India where the personal data is collected— (i) in digital form; or (ii) in non-digital form and digitized subsequently; Australian Privacy Act, 1988, subsection 2A: "The objects of this Act are: …(d) to promote responsible and transparent handling of personal information by entities; …and (f) to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected…".

Hohfeld classified jural relations into primary and secondary[80]. According to Roman law, *accessio* is – additional to the principal. With the termination of the principal obligation, the additional obligations also terminate. If the main one ceases, then the accessory one also ceases and can no longer exist. At the same time, the accessory obligation does not have a reverse effect on the principal one.

Thus, for example, when data subject participates in a contract, the principal legal relationship here is the contract itself, and an accessory will be the legal relationship of processing the data subject's personal data for the purposes of contract' execution. With the termination of the contract (the principal legal relationship), the privacy legal relationship (an accessory), that arose on its basis, will also cease. To continue processing the same personal data, a new basis will be required, to which the terminated contract can no longer serve.

Without principal legal relationships, accessory privacy legal relationships will not arise, because the first one generates legal facts for the latter one. At the same time, the accessory legal relationship follows the fate of the principal one. It means that when the principal legal relationship terminates and accessory legal relationship also terminates by it, the respective terminating legal fact will determine the expiration date of data processing. Accordingly, the data processing in accessory legal relationships terminates together with the termination of the principal legal relationship and depends on it.

The only legal basis for data processing, that straightaway creates a privacy legal relationship with the sole purpose of data processing is a consent. Considering the consent from the civil law' point of view, provision of consent is an acceptance of controller's offer of data processing, a legal fact, an act of the data subject that entails the emergence of privacy legal relationship *(Answer to question #8)*. Accordingly, revocation of consent is a legal fact that entails the termination of this relationship.

When consent is used in a natural way, its withdrawal cannot affect or lead to the termination of any *principal* legal relationship due to the absence of latter. Therefore, the particular term for the expiration of privacy legal relationship, which arose on the basis of consent, must be set by the term or event, stipulated by data controller in the text of the consent' request, or it must end with a legal fact — withdrawal of consent. Practically it means that the expiration date of data processing (i.e., the term of the consent itself) cannot be determined by any other circumstances, except for the two mentioned above. Such terminating legal facts as expiration of terms established by laws or the contract expiration – usually cease the principal legal relationships and lead to the termination of accessory legal relationships, dependent on them. Only the processing arising as accessory follows the fate of the principal legal relationship. Whereas legal relationships that arise based on consent cannot and should not be terminated as accessory. It would be nonsense (*Answer to question #9*).

Therefore, consent should not be sought from data subjects where privacy legal relationship is already accessory to some principal legal relationships i.e., where there is already a legal fact provoking the processing of personal data. In this case, another legal fact in the form of consent would be redundant. That is why "doubling" legal facts violates the stability of civil legal

[80] *See* Hohfeld, *supra* note 51, at 712.

relationships and leads to the issue when the withdrawal of consent may destroy the principal legal relationships. If consent is requested where it is initially unnecessary, an error occurs: the accessory legal relationship affects the principal one, which should be impossible. After all, the nature and logic of consent consist in initiating the legal relationship of processing personal data independently, in the absence of other legal fact (principal legal relationship) (*Answer to question #10*).

That is why, when choosing the most suitable legal basis for data processing, privacy professionals rely on a technique known as the "waterfall of legal grounds": going through all possible grounds before finally relying on consent[81]. This means that the processing of personal data may be either a "side effect" of the subject's participation in some principal legal relationships or, in the absence of principal legal relationship, be an end in itself and the only object of the subject's privacy legal relationship with the data controller. Only after exhausting all possibilities to be accessory, data processing becomes possible as a main legal relationship arising based on consent.

Thus, privacy legal relationships can be divided into principal and accessory, depending on the degree of their independence. Most of these legal relationships have a derivative, dependent nature and follow the principal.

III. Property and non-property

The next criterion for classifying privacy legal relationships is the object. Property legal relationships are formed regarding assets, rights to which can be transferred. Non-property legal relationships have such objects, rights to which are inseparable from the person.

All privacy legal relationships of data subjects are non-property, as personal data, or rather the degree of its unknowingness, established and maintained by this data subject, is a personal non-property good, inseparable from it.

Among the non-property privacy legal relationships, there are some that are still related to property legal relationships. Of course, it is impossible for data subject to sell own privacy rights, however, the provision of personal data as a payment for services has been considered not only in practice but also at the legislative level. For example, EU law recognized the possibility of a property element in non-property legal relationships: e.g. according to Recital 24 of Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter Directive 2019/770), "digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognizing that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, the Directive 2019/770 should ensure that consumers are, in the context of such business models, entitled to contractual remedies. It should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the

[81] The author of the approach is Siarhei Varankevich, CIPP/E, CIPM, CIPT, MBA, FIP, Data protection trainer and principal consultant at DPO Europe GmbH. Professional page: https://data-privacy-office.eu/person/siarhei-varankevich.

consumer, and the consumer *provides, or undertakes to provide, personal data"*. The amended version of the Directive 2011/83/EU also applies to legal relationships, where the consumer provides or undertakes to provide personal data to the trader[82] [83].

In Germany the legislative process for the implementation of these new Directives has been completed by adopting a few legal acts, introducing a variety of new requirements and obligations[84]. For example, section 312 (1a) and section 327 (3) of German Civil Code introduce the contracts, where consumer makes available personal data to the trader or enters obligation to do so. Those are service-for-data relationships. Payment with personal data is now officially a legal phenomenon.

The European legislators thus reject the idea of apparently free Internet services that actually live from the use of their users' personal data and from this generate considerable company profits. For too long, contract law has overlooked the fact that the user of advertising-financed services is by no means given a gift. Internet companies are also geared towards maximizing profits and have nothing to give away. In this respect, the often-invoked free culture on the Internet is just a backdrop[85].

Provision of personal data in exchange for receiving payment, bonus, discount, reward, gift, content, service, etc., is a non-property privacy legal relationship, which is related to a particular property legal relationship, where e.g. service provider (data controller) grants access to the service and permits its use on the basis of e.g. a license agreement to the consumer (data subject) or to a third party designated by the consumer, and the consumer in its turn fulfills contractual obligations, including provision of personal data as a renumeration. Such relationships between data subjects and data controllers form the primary data market[86]. Provision of personal data itself could be considered here as fulfillment of data subject's contractual obligation, so the subject can expect to be put in the same position as if it had paid money for the service.

Moreover, typically data subjects are obliged to only provide true and not misleading information, to use its real name and no pseudonyms or stage names and to notify of any changes to the information provided. Such obligations become enforceable only if they are clearly stipulated in the contract — e.g. in general terms and conditions.

These consumer's contractual obligations are reciprocal to the service provider's obligation to provide the service: the consumer promises its performance for the sake of others' performance.

---

[82] *See* Consolidated text: Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, art 3.1a.

[83] Still, according to Recital 25 of Directive 2019/770, if digital content and digital services are not supplied in exchange for a price, the Directive should not apply to situations where the trader collects personal data exclusively to supply digital content or a digital service, or for the sole purpose of meeting legal requirements. The similar is stipulated in Article 3 (1a) of amended Directive 2011/83/EU.

[84] Lea Noemi Mackert, *Consumer protection laws in Germany: Major updates* (2022), https://www.twobirds.com/en/insights/2022/germany/verbraucherschutzgesetze-in-deutschland-wichtige-neuerungen.

[85] Axel Metzger, *Dienst Gegen Daten: Ein Synallagmatischer Vertrag*, vol. 216 n 6 ARCHIV FÜR DIE CIVILISTISCHE PRAXIS 818 (2016).

[86] Louisa Specht, *Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit* – Eckpfeiler eines neuen Datenschuldrechts, Rheinische Friedrich-Wilhelms-Universität Bonn DGRI-Jahrbuch, 9 (2017). https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Specht_Datenschuldrecht4.pdf

This corresponds to the idea of synallagma[87], a mutual contract, where personal data serves as a counter-performance for the benefit and data subject has the right to demand its provision. The consumer (data subject) must therefore understand the corresponding clauses in the terms of use in the sense of a real contractual obligation. Also, the consumer's obligations are subject to the reservation of free revocability at any time.

Due to its participation in civil legal relationships as a means of payment, personal data is increasingly valued as a property. As Julie E. Cohen writes in her book "Between Truth and Power: The Legal Constructions of Informational Capitalism": "One important byproduct of these access-for-data arrangements is a quiet revolution in the legal status of data as (de facto if not de jure) proprietary informational property"[88].

Another layer of privacy legal relationships arises at the secondary data market[89]. Here the data controller transfers the personal data further to some data acquirer in exchange for fee or other data or services. Personal data in such legal relationships becomes an object—information, a controller's asset, property rights to which can be evaluated and transferred to a counterparty. In this case, we can talk about the emergence of a property legal relationship. Examples of usual participants of such relationships on the secondary data market are the contacts' traders, social media, web analytics services, telecom operators, internet providers, data aggregators, manufacturers of smart devices, etc.

It is important to note here that data processing arising on the basis of a remunerated contract itself, for example, employment contract, will not be a non-property legal relationship related to a property legal relationship, because the data subject receives remuneration and other benefits not as a counter-performance for providing of personal data, but for labor within the scope of labor legal relationship. Only where the data subject is compensated specifically for the provision of personal data will arise the non-property legal relationships, related to property legal relationship.

So, where personal data is a means of payment under a license or some other reimbursable agreement, and where it serves to acquiring property or non-property goods by the data subject, such legal relationships should be considered as property legal relationships. Hence, the arising from the latter privacy legal relationships should be qualified as non-property legal relationships, related to property legal relationships.

IV. Organizational

As in any other civil legal relationships, participants of privacy legal relationships often enter supporting organizational relationships which serve to organizing them.

These organizational relationships have a subordinate, accessory role in relation to the principal legal relationships that they are designed to order and normalize. For example, representation relationship, when a parent or a legal representative (also called a "proxy") represents the data

---

[87] See Metzger, *supra* note 85, at 835; See also Id at 6.

[88] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM, 44 (2019).

[89] See Specht, *supra* note 86, at 9.

subject, are designed to support the emergence and further development of the principal privacy legal relationship.

It worth mentioning here, that acting in a representative role, individual doesn't enter privacy legal relationships of its own will and in its own interest. Representative only performs the powers on principal's behalf to enable the privacy legal relationships between principal and processing participant. That's why, staying always outside of the principal's privacy legal relationships with processing participant, representative has no own privacy rights to address to the processing participant. The only legal relationships representative enters within exercising the powers, are two organizational legal relationships: one with the principal and one with the processing participant. If the processing of the representative's personal data goes beyond the minimum required for the exercising of powers, then it leaves the representative's role and begin interaction with processing participant in its own interest as a new data subject. In this case, a new relative privacy legal relationship will arise.

The succession relationship after data subject's death[90] (an element of so-called "post-mortem privacy"[91]) has also organizational character, as it aims to continue the existing privacy relationship after the death of its main protagonist. For example, according to Illinois Revised Uniform Fiduciary Access to Digital Assets Act (2015)[92] content of electronic communications and the digital assets of deceased user could be disclosed by platform to duly authorized personal representative of the user's estate. Or section 3(1)(f) of the Access to Health Records Act 1990 enables the patient's personal representative and any person who may have a claim arising out of the patient's death to access to a health record, or to any part of a health record.

Also, intravital succession relationship after change of personal data "ownership", when data itself is a part of intellectual property or digital asset of data subject, — have an organizational nature aimed at ensuring the seamless continuing and uninterrupted functioning of the principal privacy legal relationship.

Legal relationships between processing participants (as mentioned above – controllers, processors, sub-processors, joint-controllers, co-controllers, exporters, importers, etc.) are also organizational and are usually formalized in data processing or data transfer agreements, joint-controllership or data sharing agreements, etc. Those documents draws so much attention of legal and privacy professionals, but in fact, the organizational legal relationships which they embody, hardly occupy a central place in the universe of all privacy legal relationships.

It would also be fair to classify as organizational the legal relationships arising between processing participant and its employee or other representative who perform processing on its behalf. Although these legal relationships may not be formalized in a single document, they are still regulated by a multitude of scattered norms related to data processing and protection (labor or other

---

[90] Uta Kohl, *What post-mortem privacy may teach us about privacy*, Volume 47 COMPUTER LAW & SECURITY REVIEW 2 (2022); *see also* the German Criminal Code, para 189 (offence of defiling the memory of the dead).

[91] *See, e.g.,* Jason Mazzone, *Facebook's Afterlife*, 90 NORTH CAROLINA LAW REVIEW 1643 (2012); Lilian Edwards, Edina Harbinja, *Protecting PostMortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World*, 32/1 CARDOZO ARTS & ENTERTAINMENT LAW JOURNAL 101 (2013); Natalie M Banta, *Death and Privacy in the Digital Age*, 94 NORTH CAROLINA LAW REVIEW 927 (2016); FLORIS TOMASINI, REMEMBERING AND DISREMEMBERING THE DEAD Ch3 (2017).

[92] Illinois Revised Uniform Fiduciary Access to Digital Assets Act (2015), sections 7 and 8.

contract, job description, internal policies, obligation of data protection, familiarization sheets, trainings, attestations, etc.), by which data processing participant oblige its representative to process personal data in accordance with mandatory and declared characteristics of processing, under the threat of disciplinary and other liability.

The data subjects joining groups and data cooperatives also participate in organizational legal relationships within them.

It is interesting to note that privacy legal relationships, being mostly accessory, themselves — act as principal for organizational legal relationships. So being "double" accessory, the organizational legal relationship follows the fate of both principal legal relationships: e.g., when the contract with data subject is terminated, the legal relationship of data processing, based on it, also terminates and the dependent organizational legal relationship too.

V. Administrative

Processing participants and data subjects may enter privacy legal relationships with the supervisory authority (further also – authority) in the manner prescribed by laws and administrative rules, where authority exercises its powers, while other participants exercise mainly legal obligations and some limited rights.

The peculiarity of administrative legal relationship is the participation of an empowered party, and this makes administrative relationship public. Still, when authority enters privacy legal relationship as equal with the counterparty (processing participant or data subject), outside its powers, such legal relationship will rather relate to relative private legal relationship.

German juridic doctrine granulates internal public administrative legal relationships into at least four subtypes: a) management and instructions, b) monitoring, control and supervision, c) obligations, and d) collaboration (cooperation and coordination)[93]. Let's use some GDPR clauses to demonstrate how those four can be mirrored in privacy laws:

a) **management and instructions**: Article 34 Communication of a personal data breach to the data subject; Article 35 Data protection impact assessment; Article 36 Prior consultation; Article 46 Transfers subject to appropriate safeguards;

b) **monitoring, control and supervision**: Article 31 Cooperation with the supervisory authority; Article 40 Codes of conduct; Article 41 Monitoring of approved codes of conduct; Article 42 Certification; Article 47 Binding corporate rules; Article 58 Powers; Article 83 General conditions for imposing administrative fines;

c) **obligations**: Article 51 Supervisory authority; Article 52 Independence; Article 57 Tasks; Article 77 Right to lodge a complaint with a supervisory authority;

d) **collaboration (cooperation and coordination)**: Chapter 7 Cooperation and consistency.

Some data controllers find themselves involved in public administrative privacy legal relationships (further also – administrative relationships) for the entire period of data processing when authority unilaterally include them in some sort of registry, e.g. register of data controllers or register of data protection officers, to execute the controlling and supervisory powers. Also, data

[93] ANDREAS WIMMER, RECHTSVERHÄLTNISSE IM ÖFFENTLICHEN RECHT: EIN PERSPEKTIVENWECHSEL 629 (2019).

controller may find itself in administrative relationship if it violates the legal requirements or is subjected to control and supervision based on a complaint. And some data controllers are obliged to enter the administrative relationships by notification of their intention to begin data processing, or to carry out data transfer, or on the fact of data breach, etc.

Data subjects, its associations and processing participants may also enter administrative relationships by requesting some consultations from the authority. It should be noted that when data subject appeals the actions or inaction of processing participant to the authority, it initiates a public protective legal relationship, which is considered below.

VI. Normative, Protective, and Procedural

Another criterion for classifying privacy legal relationships is a degree of voluntariness of the obliged party's lawful behavior. Based on this criterion, normative[94], protective, and procedural legal relationships can be distinguished.

A privacy legal relationship is considered normative when the data controller's behavior in the relationship is both lawful and voluntary, aligning with the behavior prescribed by the legislation, policy, contract, or other obligation. In the field of informational privacy, all absolute and relative legal relationships that follow a normatively prescribed path, unaffected by violations of data subject's rights or legal norms, or non-performance or improper performance by the data controller, can be considered normative.

For instance, seemingly conflicting situations, such as the withdrawal of consent, objection to an automated decision making, or data erasure request, are addressed by the subject within a normative legal relationship that naturally develops. Here, the data controller voluntarily acts lawfully, does not infringe upon the data subject's rights, and the data subject exercises its privacy rights at its discretion.

If the data controller needs to be compelled to behave lawfully or to apply measures to protect privacy rights, a newly arisen privacy legal relationship will be protective. This relationship aims to protect the data subject's rights and remedy any violations. For instance, in case of unlawful data processing the controller must cease such processing or delete personal data at the request of the data subject, its representative or supervisory authority. Therefore, in such cases, the controller is forced to behave lawfully by the data subject or by supervisory authority.

In some cases, coercion reaches its extreme, and then the lawful behavior of the obliged party is ensured by measures of state coercion within administrative or civil proceedings. Thus, procedural legal relationships arise in the field of informational privacy, in which one of the parties is a government authority, such as a supervisory authority or a court. The degree of voluntariness of the obliged party in this case will be minimal because the realization/protection of the data subject's right or public interest in the privacy sphere has not been achieved by other means, neither within the framework of normative nor protective legal relationships.

---

[94] See FERNANDES, *supra* note 6, at 117.

Normative and protective privacy legal relationships can be civil (no party, exercising authorities) or public (one party exercise its authorities), and procedural privacy legal relationships are typically public as one of the parties is always a supervisory authority or court.

This article will not consider enforcement procedural privacy legal relationships, as it seems, that they do not have any specific features in the field of informational privacy.

VII. Privacy tort

If an absolute privacy legal relationship is violated, and one of the many undefined passive persons (individual or legal entity), opposing the data subject, determines itself by violation its passive obligation to comply with the access mode to personal data, established by data subject, a civil tort arises – the relative legal relationship between data subject and a particular defender – an *informational* privacy tort.

Violation here occurs inside a latent absolute relationship and outside of any existing relative legal relationships between the parties and may be the result of an intentional illegal or unlawful conduct (tort) or the result of unintentional non-contractual civil wrongdoing: negligence or recklessness (quasi-tort).

Some types of privacy torts are illustrated in the Taxonomy of harm[95]: disclosure, exposure, appropriation, distortion, surveillance, intrusion. The American jurisprudence on privacy classifies four types of torts: intrusion upon seclusion; appropriation of a person's name or likeness for commercial gain; public disclosure of private facts; publicity placing person in false light[96]. English law also knows such types of torts which are suitable to protect privacy: defamation, harassment, trespass to land, wrongful disclosure of private information and wrongfully obtaining access to private information.

The classic examples of *informational* privacy torts encountered in practice and concerning everyone are: data leaks, caused by employees or former employees of processing participant, aggregation of personal data without data subjects knowing, dissemination of personal data on the darknet. It is important to note here, that data leaks, caused by data controller in a relative legal relationship, does not create a tort, but lead to the emergence of relative protective or procedural legal relationship.

To understand the specific of privacy torts, let's look at the well-publicized case *Fearn and others v Board of Trustees of the Tate Gallery*[97] arose out of the ability of the Tate Modern Museum visitors to look into some flats of the nearby building from the viewing gallery of the museum. The visitors were able to make pictures or video of what's going on inside the flats, and then post it on social media. The Appellants seek an injunction requiring the museum to prevent its visitors from viewing their flats from the viewing platform, or alternatively, an award of damages.

---

[95] *See* Taxonomy of harm, *supra* note 70.

[96] William L. Prosser, *Privacy,* Vol. 48/3 CALIFORNIA LAW REVIEW 422 (1960).

[97] Case 2020/0056, *Fearn and others (Appellants) v Board of Trustees of the Tate Gallery (Respondent)* [2023] Judgement of Supreme Court: UKSC 4:2023.

It appears that in this case *at least* two types of torts happened: i) the tort of nuisance, considered by the court, and ii) the invasion of privacy, which was out of the consideration, but is of interest for this work.

The invasion of *informational* privacy here is expressed in the publication and distribution of personal data (photos and videos) by visitors. By the way, looking back at the Seven types of privacy[98], additionally to the violation of the informational privacy in this case, we can also see the violation of privacy of the person (right to keep body private), privacy of behavior and action (activities in private space), privacy of location and space (right to solitude).

As long as plaintiffs' personal data remained at visitors' personal disposal and not published, it is too early to talk about privacy tort, although according to the Taxonomy of harm[99] it is already a privacy violation in form of surveillance and intrusion (the Taxonomy does not link the types of harm to the types of privacy, but proximate to this).

As soon as plaintiffs' personal data become published/disseminated, visitors violate their passive obligation [from absolute privacy legal relationships with each plaintiff] to comply with the access mode to personal data, established by each plaintiff. By default, we assume that none of the plaintiffs would have wanted such publication or dissemination, despite living in a house with glass walls, otherwise they would not have participated in the lawsuit.

Speaking about the tort of invasion of *informational* privacy in this case, the visitors seem proper defendants, unless they proof that processing of plaintiffs' personal data was for their purely personal activity. Although visitors were not involved in this case, each of them may be sued by the data subject, whose rights to *informational* or to *other* privacy are violated. But if some of visitors haven't publish or disseminate plaintiffs' personal data, then such processing would probably fall under the so-called household exemption — processing for purely personal or household activity[100] of the visitor.

As for the museum itself, it is unlikely to be a proper defendant in the case of invasion of *informational* privacy, although we have to admit that it has created some provocative conditions for invasion of *informational* and some *other* types of plaintiffs' privacy by the visitors, what probably can be regarded as some type of negligence. Strictly speaking, to decide whether museum is a proper defendant in the case of invasion of *informational* privacy, we have to consider what kind of passive obligation the museum has to each of the plaintiffs [being in absolute legal relationship with them] and whether the museum violated it in the form of action or inaction, through an intentional illegal or unlawful conduct (tort) or the unintentional non-contractual civil wrongdoing: negligence or recklessness (quasi-tort).

Thus, although absolute legal relationships in the field of *informational* privacy exist latently and imperceptibly between all people and organizations, including friends, relatives, neighbors, passers-

---

[98] *See* Friedewald et al., *supra* note 12.

[99] *See* Taxonomy of harm, *supra* note 70.

[100] *See* Article 2 (2) (c) and Recital 18 of GDPR: "…the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity"; *See also* Article 3.c(i) of the Digital Personal Data Protection Act, 2023, India: "Subject to the provisions of this Act, it shall not apply to personal data processed by an individual for any personal or domestic purpose".

by, private and public companies, etc., and all of us coexist without thinking about our passive obligations form them, if one of us violates its obligation – a new relative legal relationship arises between specific parties, called the *informational* privacy tort.

Conclusion

As a result of the above reasoning, it becomes possible to classify privacy legal relationships into the following ten types: 1) absolute civil legal relationship; 2) relative non-property civil legal relationship; 3) relative civil non-property legal relationship, related to property legal relationship; 4) relative civil property legal relationship, 5) relative civil organizational legal relationship; 6) relative public administrative legal relationship; 7) relative normative legal relationship (public/civil); 8) relative protective legal relationship (public/civil); 9) relative public procedural legal relationship; 10) relative civil tort legal relationship. It is important to note that absolute majority of privacy relationships between individuals are unregulated due to falling under the household exemption. These privacy relationships are usually outside of legal regulation, until the moment of violation, which may provoke a corresponding protective or procedural legal relationship.

Thus, we have classified in the sphere of informational privacy six civil legal relationships, two public ones, and two legal relationships that, can be attributed to both civil and public, depending on the composition. Can we classify based on that the privacy law in general as a private or a public law? Hardly. Probably, only legal relationships, not branches of law, laws, or academic disciplines, can be distinctly classified into private or public.

Understanding the nature of existing privacy legal relationships, the logic and stable patterns of its functioning should enable the legislators to formulate the laws more consciously and to avoid granting data subjects illusory rights[101], the law enforcers – to protect data subjects' rights more effectively, and the data controllers – to refrain from the endogeneity of privacy law[102] in favor of a human-centric and fair solution to their business goals.

[101] Daniel J. Solove, *The Limitations of Privacy Rights*, 98/3 NOTRE DAME LAW REVIEW 975, 996 (2023).

[102] Ari Ezra Waldman, *Privacy Law's False Promise*, 97/2 WASHINGTON UNIVERSITY LAW REVIEW 20 (2020).