SORBONNE DOCTORAL LAW REVIEW
REVUE DOCTORALE DE DROIT DE LA SORBONNE

2024

Volume 7, N°1

Sorbonne Doctoral Law Review – Revue doctorale de droit de la Sorbonne
12 Place du Panthéon, 75005 Paris, France
Sorbonnedoctorallawreview.org
sslr@univ-paris1.fr

Publié en ligne le 19 décembre 2024.
Published online on December 19th, 2024

Advisory Board - Comité scientifique

TABLE OF CONTENT - SOMMAIRE

EDITORIAL : LA PROTECTION DES DROITS FONDAMENTAUX AU DÉFI DES RELATIONS JURIDIQUES, UNE REVUE À L'ÈRE NUMÉRIQUE

Cher lecteurs,

À une époque où le droit se trouve confronté à des enjeux technologiques, sociétales et politiques inédits, il devient impératif de repenser les relations entre droit et société. L'ère numérique, avec ses avancées vertigineuses, interroge plus que jamais la protection des droits fondamentaux, le rôle des systèmes juridiques et la nécessité d'une coopération internationale efficace.

Le présent numéro de la Revue Doctorale de Droit de la Sorbonne se veut une réflexion sur ces questions cruciales, en éclairant les transformations récentes qui redéfinissent les contours du droit international et comparé.

Dans ce contexte, les articles de ce numéro abordent des thématiques d'une actualité brûlante, reliant des enjeux de vie privée, de sécurité des données personnelles et de coopération juridique entre États. Ces sujets ne sont pas seulement des préoccupations théoriques, mais des défis pratiques auxquels les juristes sont confrontés au quotidien dans un monde de plus en plus interconnecté.

À l'heure où les informations personnelles sont devenues une ressource économique, leur protection soulève des questions fondamentales sur les rapports entre individu, État et entreprises. Cet article explore les interactions entre la vie privée et les obligations juridiques, notamment à travers l'évolution des législations telles que le Règlement Général sur la Protection des Données en Europe. En se penchant sur l'impact de ces réglementations sur les pratiques juridiques et leur mise en œuvre à l'échelle mondiale, cet article met en lumière les défis actuels en matière de protection de la vie privée, mais aussi les perspectives offertes par la coopération internationale pour renforcer cette protection dans un monde globalisé. (*PRIVACY LEGAL RELATIONSHIPS*)

L'un des enjeux majeurs de la société numérique contemporaine est sans aucun doute la protection des données personnelles. Avec la montée en puissance des technologies, de l'information et de la communication, les citoyens sont de plus en plus exposés à des risques de divulgation et d'utilisation non consentie de leurs données. L'article qui y est consacré propose une analyse approfondie de la manière dont les juridictions nationales et internationales appréhendent ce défi. Il s'intéresse notamment à l'équilibre entre sécurité, innovation, technologique et respect des libertés individuelles. Une attention particulière est portée à l'harmonisation des législations à l'échelle mondiale et aux divergences qui existent entre les systèmes juridiques, notamment européens et américains, à propos de la gestion des données personnelles. (*THE RIGHT TO PERSONAL DATA PROTECTION – A PROCEDURAL RIGHT*)

L'entraide judiciaire entre les nations est un pilier du droit international qui permet de garantir la coopération dans la résolution des litiges transnationaux. L'article correspondant examine l'évolution des mécanismes d'entraide judiciaire, en mettant l'accent sur les instruments internationaux et régionaux qui facilitent l'échange de renseignements et l'exécution des jugements à l'échelle

mondiale. Ce phénomène est particulièrement pertinent dans des domaines tels que la lutte contre le terrorisme, la fraude fiscale ou la traite des êtres humains. L'étude soulève également les questions d'efficacité, de respect des souverainetés nationales et de l'équilibre entre coopération et protection des droits humains. (*MUTUAL LEGAL ASSISTANCE, A MECHANISM ENABLING THE PROSECUTION OF TRANSNATIONAL ORGANISED CRIME: BARRIERS AND SOLUTIONS*)

Enfin, la question de l'équité dans le système juridique de la common law, en pleine mutation, occupe une place centrale dans ce numéro. L'auteur analyse la manière dont la notion d'équité, longtemps perçue comme un complément au droit strictement positif, a évolué pour devenir un principe fondamental dans la résolution des conflits. L'extension de l'équité à de nouveaux domaines, comme la régulation des pratiques commerciales ou la protection des droits sociaux, montre que le droit de la common law se réinvente constamment pour répondre aux enjeux contemporains. Cette réflexion est essentielle pour comprendre comment les systèmes juridiques peuvent s'adapter aux besoins de justice dans un monde où l'équité ne peut plus être simplement un recours, mais doit devenir une norme de régulation. (*THE DEVELOPMENT OF EQUITY UNDER THE COMMON LAW LEGAL SYSTEM: AN INTRODUCTION*)

Lors de la récente conférence sur la personnalité juridique des animaux et de l'intelligence artificielle, des débats fascinants ont été lancés sur l'élargissement des frontières de la personnalité juridique. Si les animaux ont acquis une reconnaissance juridique accrue dans certains systèmes juridiques, la question se pose désormais de savoir si l'intelligence artificielle, en constante évolution, pourrait un jour prétendre à une forme de personnalité juridique. Le rôle de l'intelligence artificielle dans les relations sociales et économiques soulève des questions de responsabilité, de droits et de régulation qui méritent également une attention particulière. La réflexion en cours sur ce sujet bouleverse les conceptions traditionnelles de la personnalité juridique et ouvre des perspectives nouvelles sur la manière dont le droit pourrait évoluer face à ces entités non humaines. Dans une dynamique de partage et de réflexion collective, nous annonçons également la tenue de notre prochaine conférence dédiée au parcours doctoral en droit : le parcours doctoral en droit et l'avenir de la recherche juridique. Ce sera une occasion unique d'entendre des doctorants et des professionnels du droit échanger sur l'évolution de la recherche juridique, les défis auxquels font face les jeunes chercheurs et l'impact de leurs travaux sur le droit contemporain. Cette conférence visera à favoriser un dialogue interdisciplinaire et à stimuler les réflexions sur l'avenir du droit, à travers les perspectives des chercheurs en herbe, des praticiens et des universitaires aguerris.

En Conclusion, les articles présentés dans ce numéro de la Revue Doctorale de Droit de La Sorbonne soulignent l'importance de repenser les rapports entre droit et société à travers une approche critique et interdisciplinaire. La protection de la vie privée, l'entraide judiciaire internationale, la régulation des données personnelles et l'évolution de l'équité dans la common law ne sont pas des sujets isolés. Au contraire, ils s'inscrivent dans un cadre global où les frontières entre les systèmes juridiques se brouillent, où les défis dépassent les compétences nationales et où les principes fondamentaux de justice et de droits humains doivent guider chaque révision des normes. C'est cette quête d'équilibre

entre protection des libertés individuelles et efficacité juridique qui définit les grandes questions auxquelles les juristes devront répondre dans les décennies à venir. Ce numéro invite ainsi à une réflexion en profondeur sur les enjeux contemporains du droit et à une exploration de nouvelles pistes pour garantir un avenir juridique qui soit à la fois plus équitable, plus protecteur des libertés et plus respectueux des principes de coopération internationale. Il met en lumière des sujets d'une grande portée, qui façonnent le paysage juridique international et comparé d'aujourd'hui. Ils offrent également une occasion unique de réinventer le droit, de l'adapter aux réalités contemporaines et de garantir une justice plus équitable et plus respectueuse des libertés fondamentales dans un monde en constante évolution.

Nous vous invitons à poursuivre cette réflexion au travers des articles et à nous rejoindre lors de nos événements futurs, pour continuer à construire ensemble un avenir juridique plus juste et plus inclusif.

EDITORIAL : THE PROTECTION OF FUNDAMENTAL RIGHTS IN LEGAL RELATIONS: A REVIEW FOR THE DIGITAL AGE

Dear Readers,

At a time when the law is facing unprecedented technological, societal and political challenges, it is becoming imperative to rethink the relationship between law and society. The digital age, with its dizzying advances, raises questions more than ever about the protection of fundamental rights, the role of legal systems and the need for effective international cooperation.
This issue of the Sorbonne Doctoral Law Review aims to reflect on these crucial issues, shedding light on recent transformations that are redefining the contours of international and comparative law.
Against this backdrop, the articles in this issue address highly topical themes, linking issues of privacy, personal data security and legal cooperation between States. These topics are not just theoretical concerns, but practical challenges that lawyers face on a daily basis in an increasingly interconnected world.

At a time when personal information has become an economic resource, protecting it raises fundamental questions about the relationship between the individual, the state and companies. This article explores the interactions between privacy and legal obligations, particularly through the evolution of legislation such as the General Data Protection Regulation in Europe. By looking at the impact of these regulations on legal practices and their implementation on a global scale, this article highlights the current challenges in terms of privacy protection, but also the prospects offered by international cooperation to strengthen this protection in a globalized world. (*PRIVACY LEGAL RELATIONSHIPS*)
One of the major challenges of today's digital society is undoubtedly the protection of personal data. With the rise in power of information and communication technologies, citizens are increasingly exposed to risks of disclosure and non-consensual use of their data. This article provides an in-depth analysis of how national and international jurisdictions are tackling this challenge. In particular, it looks at the balance between security, innovation, technology and respect for individual freedoms. Particular attention is paid to the harmonization of legislation on a global scale, and to the divergences that exist between legal systems, particularly in Europe and the USA, with regard to the management of personal data. (*THE RIGHT TO PERSONAL DATA PROTECTION - A PROCEDURAL RIGHT*)
Mutual legal assistance between nations is a pillar of international law that ensures cooperation in the resolution of transnational disputes. The corresponding article examines the evolution of mutual legal assistance mechanisms, focusing on international and regional instruments that facilitate the exchange of information and the enforcement of judgments on a global scale. This is particularly relevant in areas such as the fight against terrorism, tax fraud and human trafficking. (*MUTUAL*

LEGAL ASSISTANCE, A MECHANISM ENABLING THE PROSECUTION OF TRANSNATIONAL ORGANIZED CRIME: BARRIERS AND SOLUTIONS)

Last but not least, the issue of equity in the evolving common law legal system takes center stage in this issue. The author analyzes how the notion of equity, long perceived as a complement to strictly positive law, has evolved to become a fundamental principle in conflict resolution. The extension of equity to new fields, such as the regulation of commercial practices or the protection of social rights, shows that common law is constantly reinventing itself to meet contemporary challenges. This reflection is essential to understanding how legal systems can adapt to the needs of justice in a world where equity can no longer be simply a recourse, but must become a standard of regulation. (*THE DEVELOPMENT OF EQUITY UNDER THE COMMON LAW LEGAL SYSTEM: AN INTRODUCTION*)

At the recent conference on the legal personality of animals and artificial intelligence, fascinating debates were launched on expanding the boundaries of legal personality. While animals have gained increased legal recognition in some legal systems, the question now arises as to whether the ever-evolving artificial intelligence could one day lay claim to some form of legal personality. The role of artificial intelligence in social and economic relations raises questions of responsibility, rights and regulation that also deserve particular attention. Current thinking on this subject is overturning traditional conceptions of legal personality, and opening up new perspectives on how the law might evolve in the face of these non-human entities. In a spirit of sharing and collective reflection, we are also announcing our next conference dedicated to the doctoral path in law: the doctoral path in law and the future of legal research. This will be a unique opportunity to hear doctoral students and legal professionals discuss the evolution of legal research, the challenges facing young researchers and the impact of their work on contemporary law.

This conference will aim to foster interdisciplinary dialogue and stimulate reflection on the future of law, through the perspectives of budding researchers, practitioners and seasoned academics.

In conclusion, the articles presented in this issue of the Revue Doctorale de Droit de La Sorbonne underline the importance of rethinking the relationship between law and society through a critical, interdisciplinary approach. The protection of privacy, international mutual legal assistance, the regulation of personal data and the evolution of equity in common law are not isolated subjects. On the contrary, they are part of a global framework where the boundaries between legal systems are blurring, where challenges transcend national jurisdictions, and where the fundamental principles of justice and human rights must guide every revision of standards.

It is this quest for balance between the protection of individual freedoms and legal efficiency that defines the major questions that legal scholars will have to answer in the decades to come. This issue invites us to reflect in depth on contemporary legal issues, and to explore new ways of ensuring a legal future that is fairer, more protective of freedoms and more respectful of the principles of international cooperation. It highlights far-reaching issues that are shaping today's international and comparative legal landscape. They also offer a unique opportunity to reinvent the law, to adapt it to

contemporary realities, and to ensure that justice is more equitable and more respectful of fundamental freedoms in an ever-changing world.

We invite you to pursue this reflection through the articles and to join us at our future events, so that together we can continue to build a fairer and more inclusive legal future.

Privacy Legal Relationships

Elena Sebiakina

SORBONNE DOCTORAL LAW REVIEW
REVUE DOCTORALE DE DROIT DE LA SORBONNE
Vol. 7 n°1

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.

---

[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).

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 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.

---

[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).

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 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

---

[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.

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].

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

---

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).

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).

relations[26] or relationship of trust[27]) or as a collective interest (associational privacy[28], group 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,

---

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.

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).

"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].

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,

---

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.

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).

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.

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.

---

[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.

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.

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

---

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).

"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].

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

---

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).

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.

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.

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

---

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

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

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

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

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 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

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

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

---

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)).

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.

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*).

---

[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)).

[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).

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.

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 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

---

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

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.

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 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

---

[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…".

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.

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*

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

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 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.

---

[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.

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 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

---

[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).

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. 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

---

[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

[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.

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 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

---

[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.

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 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 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

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

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

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.

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.

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).

---

[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.

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

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

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-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

[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".

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).

The Right to Personal Data Protection – A Procedural Right

Rafael Tedrus Bento

SORBONNE DOCTORAL LAW REVIEW
REVUE DOCTORALE DE DROIT DE LA SORBONNE
Vol. 7 n°1

TABLE DES MATIERES

Résumé

Cet article vise à définir le concept de droit à la protection des données à caractère personnel. À cet égard, il est important d'examiner les exigences formelles du droit à la protection des données à caractère personnel, à savoir le sujet, le contenu et l'objet. Ainsi, le domaine juridique devrait bénéficier grandement de cette recherche, notamment en raison du débat intense entourant la mise en œuvre du système mondial de protection des données à caractère personnel. En outre, ce travail académique cherche à identifier les modèles normatifs et les caractéristiques du droit fondamental en question. Il se situe donc dans le domaine de la dogmatique juridique. Pour répondre à ces questions, cette étude propose une exploration de la conception de la protection des données personnelles, en analysant ses origines et le développement de sa conception jusqu'à aujourd'hui. Il s'agit donc d'une étude de l'évolution de la compréhension de ce droit. Ainsi, nous pouvons définir les objectifs de cette thèse comme suit : (i) élucider la construction du droit à la protection des données personnelles, en considérant les exigences intrinsèques du droit subjectif fondamental ; (ii) identifier les exigences de propriété, d'objet et de contenu du droit subjectif actuel. Pour répondre à ces questions, cette étude sera structurée comme suit. Dans la première partie, un bref historique de la discussion sur le droit à la protection des données à caractère personnel et des sujets fréquemment liés sera fourni. Dans la deuxième partie, une analyse plus détaillée des concepts de vie privée, d'information et de protection des données personnelles sera présentée.

Abstract

This article aims to identify the concept of the Right to Personal Data Protection. In this regard, it is important to examine the formal requirements of the right to personal data protection, namely, subject, content, and object. Thus, the legal field stands to benefit greatly from this research, particularly given the intense debate surrounding the implementation of the global system for the protection of personal data. Furthermore, this academic work seeks to identify normative patterns and characteristics of the fundamental right in question. It is therefore situated within the field of legal dogmatics. To address these issues, this study proposes an exploration of the conception of personal data protection, analyzing its origins and the development of its conception to the present moment. It is, therefore, a study of the evolution of the understanding of this right. Thus, we can define the objectives of this thesis as follows: (i) To elucidate the construction of the right to personal data protection, considering the intrinsic requirements of the fundamental subjective right; (ii) To identify the requirements of ownership, object, and content of the current subjective right. To seek answers to these questions, this study will be structured as follows. In the first section, a brief history of the discussion on the right to personal data protection and frequently related topics will be provided. In the second part, a more detailed analysis of the concepts of privacy, informational self-determination, and the pursuit of an understanding of the right to personal data protection will be

conducted. In the third stage, an examination of legislation and examples of jurisprudence in the United States of America will be undertaken. In the fourth part, an analysis of the scope and limits of this fundamental right will be conducted, as well as an exploration of the understanding of the creation of due informational process and its connection to the right to personal data protection. In the fifth and final section, the "procedural" dimension of the right to personal data protection will be examined, with the aim of understanding the subjective and objective dimensions of the right, the potential essence of the right to personal data protection, and whether the right can be considered instrumental/procedural to ascertain whether the hypotheses described above are equivalent to the right pursued here.

Keywords: Personal Data Protection; Fundamental Right; Informational Self-Determination; Due Informational Process.

Introduction

The importance of determining the contours of this right has been renewed by events and debates brought forth in the 21st century, especially after 2010. Data leaks and public and private scandals, such as those revealed in the episode of unauthorized data sharing between Facebook and Cambridge Analytica[103], make clear the timeliness of the discussion on personal data protection. Websites make available the history of personal data exposed irregularly around the world.[104] In his 2023 State of the Union address, President of the United States of America, Joe Biden, criticized the practices of personal data collection by Big Tech and the use of targeted ads to young users.[105] A society constantly surveilled and monitored, individuals identified in the minutiae of their personal lives, the power of personal data controllers renewed and multiplied with automated data collection.[106] Furthermore, approximately 65% of the world's GDP has been linked to the perspective of cross-border flows of personal data.[107]

All these factors lead to the same question being constantly and insistently repeated: after all, what does it mean and what are the limits of the right to personal data protection? The exercise of reflection by this work proves necessary as it provides an opportunity to revisit key concepts of the personal data protection regime, serving as anticipation of legal and practical problems common to all nationals or internationals who propose to address this matter.

In this regard, it is important to examine the formal requirements of the right to personal data protection, namely, subject, content, and object.[108] Thus, the legal field stands to gain from this research, especially given the intense debate regarding the implementation of the national system for personal data protection. Furthermore, this academic work seeks to identify normative patterns and

---

[103] Isaak, J. and Hanna, M. J. (2018) "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer*, 51(8), pp. 56–59.

[104] Fell, J. *et al.* (2023) "See your identity pieced together from stolen data," *ABC News*, 17 May. Available at: https://www.abc.net.au/news/2023-05-18/data-breaches-your-identity-interactive/102175688 (Accessed: February 19, 2024).

[105] *State of the union 2023* (2023) *The White House*. Available at: https://www.whitehouse.gov/state-of-the-union-2023 (Accessed: February 19, 2024).

[106] Zuboff, S. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. London, England: Profile Books.

[107] Leighton, L. (2013) "No title," in, pp. 1–1.

[108] Ferraz Júnior, T. (1993) "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado," *Revista da Faculdade de Direito, Universidade de São Paulo*, 88.

characteristics of the fundamental right in question. It is therefore situated within the field of legal dogmatics. It should be noted that we use the term, as defined by Tércio Sampaio Ferraz Júnior, namely, "legal dogmatics as a means of legal work concerned with the identification of normative patterns and their respective evaluation and systematization."[109] Legal dogmatics is a way to facilitate legal understanding to society, simplifying complexity and seeking to stabilize society.[110]

Thus, we can define that the objective of this article is to expose the construction of the right to personal data protection, regarding the essential requirements of the subjective right. It is reaffirmed, therefore, that it is not seeking a complete analysis of personal data protection, but merely an attempt to construct the history of this right.

1. **Contours of the Privacy Concept**

This chapter will address the study of personal data protection and its intersections with the right to privacy. The right to privacy has emerged in countries worldwide in differents dimensions. The term "privacy" is used to refer to many different human values, including control over personal information, fairness, personal security, financial security, peace and tranquility, autonomy, integrity against commodification, and reputation.[111]

The interactions between these values and different types of information technology are complex; therefore, interventions aimed at protecting these values vary in their effectiveness and timing.[112] Privacy is used to describe many different human values. The strongest sense of privacy can be discussed as control over access to personal information, which people use to shape their personalities and roles in society.[113]

---

[109] Ferraz Júnior, T. (1993) "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado," *Revista da Faculdade de Direito, Universidade de São Paulo*, 210.

[110] Ferraz Júnior, T. (1993) "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado," *Revista da Faculdade de Direito, Universidade de São Paulo*, 200.

[111] Rigaux, F. (1991) "La liberté de la vie privée," *Revue internationale de droit comparé*, 43(3), pp. 539–563. doi: 10.3406/ridc.1991.2290.

[112] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[113] Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

The presence of information and communication networks in social, legal, and political environments has determined awareness and the need to conceive the values and rights of individuals as universal guarantees for their integral development by virtue of their essential dignity.[114] As a result of the phenomenon of datafication, which is the existence of a digital biography, which is a logical and expected result of the extension of the person through their data.[115]

In this sense, personal data not only characterize themselves as an extension of the person (subjectivity) but also influence this relational perspective of the person (intersubjectivity). The protection of personal data is instrumental for the person to freely develop their personality.[116]

The strong and growing demand for transnational alignment of regulations on privacy and data protection aims primarily to create equitable rules in an increasingly globalized world, with the intention of abstaining individuals from possible "tax havens", places where there would be no discipline of protection rights, which would enable unregulated commerce.[117]

It is important to consider, however, that beyond this bit capture of the human being, there is their classification and segmentation based on such information. True stereotypes are created that stigmatize a subject before their peers. This factor is crucial for calibrating a series of decisions that influence the course of their own lives.[118]

Automated decisions[119] based on such stereotypes of people are already a reality, and are even the subject of explicit approach by the European Union Regulation (GDPR).[120] Specifically the

---

[114] Silva, L. L. (no date) *Globalização das Redes de Comunicação: uma reflexão sobre as implicações cognitivas e sociais*.

[115] Solove, D. J. (2005) "The digital person and the future of privacy," in *Privacy and Technologies of Identity*. New York: Springer-Verlag, pp. 3–13.

[116] Solove, D. J. (2005) "The digital person and the future of privacy," in *Privacy and Technologies of Identity*. New York: Springer-Verlag, pp. 3–13.

[117] Bennett, C. (no date) *Regulating Privacy, Data protection and public policy in Europe and the United States*.

[118] Solove, D. J. (2005) "The digital person and the future of privacy," in *Privacy and Technologies of Identity*. New York: Springer-Verlag, pp. 3–13.

[119] Renato Leite Monteiro defined the term as follows: "The concept of automated decision-making can be constructed here as a result of processing personal data, without significant involvement of a human operator, computationally or otherwise, that produces or can produce effects on the individual and whose processing of the data in question allows for other possible outcome. (Monteiro, R. (no date) *Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil. 385f. Tese Doutorado. Programa de Pós-Graduação em Filosofia do Direito e Teoria Geral do Direito*).

[120] Pariser, E. (2012) *Filter Bubble: Wie wir im Internet entmündigt werden*. Translated by U. Held. Munich, Germany: Hanser.

item 22(3), in the cases outlined in subparagraphs "a" and "c," grants individuals subject to automated decisions the right to have their rights, freedoms, and legitimate interests safeguarded. Precisely, this includes the right to obtain human intervention from the responsible party, express their viewpoint, and contest the decision.

As can be observed, the GDPR[121] - more specifically in articles 13(2)(f), 14(2)(g), 15(1)(h) and 22(3) - does not explicitly or bindingly establish a "right to explanation," despite mandating practices and rights related to transparency and the right to review.[122] The notion of a right to explanation has been supported by some scholars based on a holistic interpretation of the regulation's text, particularly through a systematic reading of Articles 13, 14, 15, and 22, as well as Recital 71[123]. Although Recital 71 is not legally binding, it explicitly broadens the safeguards of Article 22(3) by stipulating a "right to explanation" in the context of automated decisions. Articles 13 and 14 encompass a set of transparency obligations, while Article 15 establishes a right of access.[124] Together, these provisions require that meaningful information be provided about the existence of automated decision-making, including profiling. Thus, the right to explanation in the GDPR would be derived from the rights and guarantees against being subject to automated decisions (Article 22(1) and (3)), as well as from the notification and information duties of controllers and the right of access (Articles 13-15).[125]

In summary, proponents assert unequivocally that the GDPR, by establishing the right to information regarding the logic behind automated decision-making processes, clearly grants a right to explanation. This right should be interpreted to enable data subjects to exercise their rights as

---

[121] JANSSEN, J. H. N. means for 'white-boxing' the black-box?: research into the ability of the 'right to explanation' about decisions based solely on automated decision-making of Articles 13(2)(f), 14(2)(g), 15(1)(h) and 22(3) of the General Data Protection Regulation, as well as of current explanation methods, to solve the legal problems arising from algorithmic decision-making. JANSSEN, J. H. N. (2012) *The right to explanation:* (Masters Thesis in Law and Technology) — Universiteit van Tilburg, Tilburg, 2019.

[122] SELBST, A. D.; POWLES, J. (2017) Meaningful Information and the Right to Explanation. *International Data Privacy Law*, v. 7, n. 4, p. 233-242.

[123] "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child."

[124] CASEY, B.; FARHANGI, A.; VOGL, (2018) R. Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise. In: *Berkeley Technology Law Journal*, v. 34, p. 145-189.

[125] GUNST, H. (2017) *The Right to Explanation and the Right to Secrecy* – Reconciling Data Protection and Trade Secret Rights in Automated Decision-making. 2017. Dissertation (Masters Thesis in Law) – Faculty of Law, University of Helsinki.

outlined in the regulation and the broader legal framework.[126] Conversely, opponents argue that the absence of the term "explanation" in the binding text of the GDPR precludes the definitive affirmation of such a right.[127]

It is the practice known as profiling, in which an individual's personal data forms a profile about them for making numerous decisions.[128] Everything is calibrated based on these stereotypes, including the content accessed on the Internet.

Eli Pariser reports that there is a bubble that - like an invisible filter - directs everything from the user's interaction with other people on a social network to accessing and searching for information on the web.[129]

The information society prints a new dynamic and new challenges for the protection of the human person, starting with the monetization of their personal data. Such data, in addition to consolidating a new form of extension of the person, begin to interfere in their own relational sphere, requiring specific standardization that dogmatically justifies the autonomy of the right to the protection of personal data and the unfolding of its legal protection.[130]

And, for this, it is necessary to seek the concepts of these rights to verify which aspects of their regulation and how the application of these rights can occur. According to the parameters set out by Rachel L. Finn and others, privacy is treated by various aspects, but it is possible to select seven (seven) subspecies, which although they have aspects of convergence, highlight unique aspects in the defense of privacy, these are (i) privacy of the person, (ii) privacy of behavior and action, (iii) privacy of personal communication, (iv) privacy of data and image, (v) privacy of thoughts and

---

[126] WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. (2017) Why a Right to Explanation of Automated Decision Making Does Exist in the General Data Protection Regulation. *In: International Data Privacy Law*, vol. 7, n. 2, maio 2017, p. 76–99.

[127] SELBST, A. D.; POWLES, (2017) J. Meaningful Information and the Right to Explanation. *International DataPrivacy Law*, v. 7, n. 4, p. 233-242.

[128] Rubinstein, I., Lee, R. D. and Paul, M. (no date) *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*

[129] Pariser, E. (2012) *Filter Bubble: Wie wir im Internet entmündigt werden*. Translated by U. Held. Munich, Germany: Hanser.

[130] Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

feelings, (vi) privacy of location and space, and (vii) privacy of association (including group privacy).[131]

Although these seven types of privacy may overlap, they are discussed individually because they provide different aspects through which the practical aspects of this right can be visualized.

The privacy of the person encompasses the right to keep the functions and characteristics of the body private (such as genetic codes and biometrics). The human body has a strong symbolic dimension because of the integration of the physical body and the mind and is intrinsic to the cultural values of society.[132] It is thought that the privacy of the person leads to individual feelings of freedom and helps support a well-adjusted democratic society.[133]

The notion of privacy of behavior and action includes sensitive issues such as sexual preferences and habits, political activities, and religious practices.[134] However, the notion of privacy of personal behavior pertains to activities that occur in public space as well as in private space. It is necessary, therefore, to make a distinction between casual observation of the behavior of nearby people in a public space, with the systematic recording and storage of information about these activities. The ability to behave in public or private space without actions being monitored or controlled by others contributes to the development and exercise of autonomy and freedom of thought and action.[135]

Privacy of communication aims to prevent the interception of communications, including mail interception, use of directional microphones, telephone or wireless communication interception, or recording and access to email messages.[136] This right is recognized by many governments, as telephone wiretaps or other communication interceptions must be supervised by an independent judicial authority. This aspect of privacy benefits individuals and society itself because it allows and

---

[131] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[132] Mordini, E. (2011) *Whole body imaging at airport checkpoints: The ethical and political context*.

[133]Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[134] Allen, A. L. (no date) *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*.

[135] Rigaux, F. (1991) "La liberté de la vie privée," *Revue internationale de droit comparé*, 43(3), pp. 539–563. doi: 10.3406/ridc.1991.2290.

[136] Poscher, R. (2017) "The right to data protection: A no-right thesis," in Miller, R. A. (ed.) *Privacy and Power*. Cambridge: Cambridge University Press, pp. 129–142.

encourages the free discussion of a wide range of views and options and enables growth in the communications sector.[137]

The category of privacy of personal data includes, but is not limited to, image capture, as they are considered a type of personal data by the European Union as part of the General Data Protection Regulation (2016/679) - especially Recitals 14, 51, article 9(1) .[138] This privacy of data and image includes concerns about ensuring that individuals' data is not automatically available to other individuals and organizations, in order to limit the exercise of control over that data. Transparency about data control increases trust in the reliability, accountability, and privacy practices of the entities managing the data. It signifies a commitment to openness and fairness, reassuring individuals that their personal information is not being misused or exploited. This transparency cultivates a sense of security and confidence, strengthening the relationship between individuals and data controllers while empowering individuals to exercise greater autonomy over their data in relation to the controller..[139]

Like privacy of thoughts and feelings, this aspect of privacy has social value, as it deals with the balance of power between the State and the individual. New technologies have the potential to impact people's privacy of thoughts and feelings. People have the right not to share their thoughts or feelings or to have those thoughts or feelings revealed.[140]

Privacy of thought and feeling can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body.[141] Similarly, we can distinguish between thought, feelings, and behavior, since thought does not automatically translate into behavior, just as one can behave without thinking.

According to the conception of privacy of location and space, individuals have the right to move in public spaces without being identified, tracked, or monitored.[142] This conception of privacy

---

[137] Raab, C. (2011) *Protecting Information Privacy. Equality and Human Rights Commission Research Report series*.

[138] Coppel, P. (2020) *Information Rights: A Practitioner's Guide to Data Protection, Freedom of Information and other Information Rights*.

[139] Paul and Gutwirth, S. (2009) *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*.

[140] Rigaux, F. (1991) "La liberté de la vie privée," *Revue internationale de droit comparé*, 43(3), pp. 539–563. doi: 10.3406/ridc.1991.2290.

[141] Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

[142] Mordini, E. (2011) *Whole body imaging at airport checkpoints: The ethical and political context*.

also includes the right to be alone and the right to privacy in private spaces such as home, car, or office. This conception of privacy has primary social value.[143] When citizens are free to move through public space without fear of identification, monitoring, or tracking, they experience a feeling of living with freedom.[144]

The final type of privacy, namely, association privacy (including group privacy), concerns the right of people to associate with whom they wish without being monitored.[145] This has long been recognized as desirable for society, as it promotes freedom of expression, including political speech, freedom of worship, and other forms of association.[146] Society benefits from this type of privacy in that a wide variety of interest groups will be promoted, which can help ensure that marginalized voices are heard.

One may question what the difference is between location and space privacy and behavior privacy. Location privacy means that a person has the right to travel through physical space, to travel where they want without being tracked and monitored.[147] Behavior privacy means that the person has the right to behave as they wish, as long as the behavior does not harm another person.[148]

Association privacy differs from behavior privacy because it is not only about groups or organizations (e.g., political parties, unions, religious groups, etc.) that we choose to belong to, but association privacy also relates to groups or profiles over which we have no control, for example, DNA testing may reveal that we are members of a particular ethnic group or a particular family.[149] Association privacy is directly related to other fundamental rights, such as freedom of religion, freedom of assembly, etc., of which behavior and action privacy is a step forward.

The primary concept of privacy was strictly linked to intimate matters, the right to secrecy, confidentiality, and isolation, thus it could be defined as a right of negative exercise, i.e., the person

---

143 Allen, A. L. (2000) *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*.

144 Finn, R. L. *et al.* (2013) *European Data Protection: Coming of Age*. Org.; London: Springer.

145 Bellanova, R., Hart, D. E. and Paul, G. (2011) "The German Constitutional Court Judgment."

146 Hildebrandt, M. (2020) *Law for computer scientists and other folk*. London, England: Oxford University Press.

147 Mordini, E. (2011) *Whole body imaging at airport checkpoints: The ethical and political context*.

148 Kokott, J. and Sobotta, C. (2013) "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR," *International data privacy law*, 3(4), pp. 222–228. doi: 10.1093/idpl/ipt017.

149 De Andrade, N. N. (2011) *Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization*.

has the right not to be invaded in their intimacy.[150] The right to privacy, therefore, also concerns interference with bodily integrity, home, and correspondence.

It is important to note that in 1960, William L. Prosser summarized the 04 (four) types of privacy harms that can cause harm to the person, namely, (i) intrusion into the plaintiff's seclusion; (ii) public disclosure of embarrassing private facts about the plaintiff; (iii) publicity that places the plaintiff in a false light in the eyes of the public; (iv) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[151] Indeed, this definition is used by most existing Courts in the United States of America to the present day.[152]

In the so-called "golden age of privacy" (the second half of the 19th century), privacy followed a path to perform the function of a right considered a prerequisite for the exercise of other fundamental freedoms, such as freedom of expression and freedom of thought, at a time when there was a growth in classical legal liberalism thought.[153]

Subsequently, it was seen that personality rights, including the concept of privacy, entered legal systems, receiving, in this context, the designation of public freedoms. The main declarations that dealt with the subject, in chronological order, were the Magna Carta (1215), the Bill of Rights (1689), the American Declaration of the Rights and Duties of Man and the Universal Declaration of Human Rights (1948).[154]

It is worth mentioning that privacy has always been considered and studied in cases related to the upper (wealthy) classes of society at that time, as in the case called "Affaire Rachel", which clearly has a causal nexus with the greater social connotation that the wealthy social classes had at the time and the society's knowledge of their right to privacy. To better explain the case, it is worth remembering that in 1858, the right to privacy was recognized for the first time in France, in case

---

[150] Bible, J. D. and McWhirter, D. (1992) *Privacy as a constitutional right: Sex, drugs, and the right to life*. Westport, CT: Praeger.

[151] Prosser, W. L. (1960) “Privacy,” *California law review*, 48(3), p. 383. doi: 10.2307/3478805.

[152] Solove, D. J. (2010) *ProsserProsser's priv's privacy law: A mixacy law: A mixed legacy ed legacy*, *Gwu.edu*. Available at: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2104&context=faculty_publications (Accessed: February 19, 2024).

[153] Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

[154] Dworkin, R. M. (1986) *A Matter of Principle*. London, England: Oxford University Press.

law, when the Séné Court recognized, to the family of a deceased actress, the right not to publish her image, on her deathbed.[155]

Furthermore, privacy began to be exercised positively by society, as a result of the detachments of the generations of fundamental rights[156], the change in the relationship between citizen and State and between citizen and companies[157], as well as the advancement of technological development, causing a greater flow of information globally and broadly. Note that privacy had its first mention in international declarations in 1948 when drafting the American Declaration of the Rights and Duties of Man, approved by the newly created Organization of American States, and the Universal Declaration of Human Rights, approved by the United Nations.[158]

In the European Union, the Charter of Fundamental Rights of the European Union addresses the topic in its article 7, specifically on the right to "respect for private and family life".[159] Indeed, privacy is considered a fundamental human right.[160] Therefore, true privacy is a product of personal responsibility. It is protected by remaining silent, refusing to interact, and keeping to oneself what is one's own concern. As a practical example, we refer to the judgments in cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources) addressed the balance of rights concerning data collection and retention by Member States. This precedent is pivotal and warrants careful analysis for the consolidation of this right within the Union. The controversy revolved around Directive 2006/24/EC, which obligated Member States to enact laws requiring internet and telecommunications providers to retain metadata of all their customers for up to two years, for law enforcement and public security purposes. The data retained under Directive 2006/24/EC could reveal personal information such as identity, time,

---

155 Sampaio, J. A. L. (1998) *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte*. Del Rey Books.

156 Bobbio, N. (1 outubro 2018) *ESTADO, GOBIERNO Y SOCIEDAD: por una teoria general de la politica*. 2nd ed. Fondo de Cultura Economica.

157 Bonavides, P. (2008) *Curso de Direito Constitucional*. 22nd ed. Malheiros Editores.

158 Doneda, D. (2019) *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*.

159 Carta D O S Direitos Fundamentais, da U. E. (no date) *7.6.2016 Jornal Oficial da União Europeia C 202/389*, *Europa.eu*. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR (Accessed: February 19, 2024).

160 Anderson, D. A. (1998) *The failure of American privacy law*, *Utexas.edu*. Available at: https://law.utexas.edu/faculty/publications/1999-The-Failure-of-American-Privacy-Law (Accessed: February 19, 2024).

location, and frequency of communication, enabling precise conclusions about individuals' private lives, including residence, movements, and social circles.[161] The Court was asked to examine the validity of Directive 2006/24/EC in light of Articles 7, 8, and 11 of the Charter of Fundamental Rights of the European Union, which concern privacy, data protection, and freedom of expression. In its decision, the Court emphasized that the essence of the right to privacy was respected since the Directive did not allow access to the content of communications. It also stated that this norm did not affect the essence of the right to personal data protection, as the Directive prescribed certain principles of data protection and security, such as technical and organizational measures against accidental or unlawful destruction, accidental loss, or alteration of data.[162]

The right to be left alone was defined in the United States in 1888 by American jurist Thomas Cooley and later solidified by Samuel Warren and Louis D. Brandeis, according to the article titled "Right to Privacy," which depicted the right to privacy in the face of photographic activity, in 1890. Through this facet of privacy, what is called in English zero-relationship is defended, that is, the total absence of interaction or relationship with the other.[163]

The United States of America provide reflective protection against violations of the right to privacy since neither its Constitution nor the Amendments to the U.S. Constitution of 1791 (known as the Bill of Rights) explicitly referred to the right to privacy. However, the Supreme Court of the United States has interpreted articles of the Bill of Rights as safeguards of an individual's right to privacy, notably based on the Fourth Amendment.[164]

The first relevant case to bring this interpretation to the American Constitution was the ruling of Griswold v. Connecticut, 381 U.S. 479 (1965), by the Supreme Court. This right to privacy has been the justification for decisions involving a wide range of civil liberty cases, including Pierce v. Society of Sisters, 268 U.S. 510 (1925), which invalidated a 1922 Oregon initiative that required compulsory public education; Roe v. Wade, 410 U.S. 113 (1973), which authorized abortion in Texas

---

[161] BOEHM, Franziska; COLE, Mark D. (2014) *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine.

[162] Case C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung and others*. Decision on April 8th 2014.

[163] Warren, S. D. and Brandeis, L. D. (1890) “The right to privacy,” *Harvard law review*, 4(5), p. 193. doi: 10.2307/1321160.

[164] Beaney, W. M. (1966) “The right to privacy and American law,” *Law and contemporary problems*, 31(2), p. 253. doi: 10.2307/1190670.

and restricted the state's excessive powers over this act; and Lawrence v. Texas, 539 U.S. 558 (2003), which struck down a sodomy law in Texas and thereby eliminated the state's powers to criminalize acts of same-sex and consenting adults.[165]

In this regard, we see the distinguished Pontes de Miranda affirming, in the 1970s, that privacy would be the fundamental basis of personal life, since there is only the right to protect private life, as there is the freedom to express it, starting from the individual will. For this significant author, the right to value intimacy would be the right to remain in reserve from the public, not to let others intrude on their private life.[166]

In a study dedicated to the origins of the privacy concept, Daniel J. Solove observed that this right was strictly linked to the protection of intimate matters, the right to secrecy, confidentiality, and isolation. Therefore, in its origin, it is an individual right of a negative nature, which recognizes the person the faculty not to be invaded in what concerns solely and exclusively to personal sphere and private life.[167]

This exclusivist conception dates to the well-known article by Samuel Warren and Louis Brandeis, in which the authors argue for the existence of a common law principle that protects privacy from unauthorized intrusions, including theft and physical appropriation, and that does not equate to private property: the inviolability of personality and privacy, or privacy.[168] In this sense, Solove recalled that the U.S. Supreme Court - decades after the publication of Warren and Brandeis' article - debated a classic case about citizens' privacy.[169]

The case known as Olmstead v. United States established that government wiretapping was not a violation under the Fourth Amendment of the U.S. Constitution since it could not be considered a physical trespass into the home. However, Justice Brandeis dissented, stating that the framers of the

---

[165] Beaney, W. M. (1966) "The right to privacy and American law," *Law and contemporary problems*, 31(2), p. 253. doi: 10.2307/1190670.

[166] de Miranda, F. C. P. (1 janeiro 2000) *Tratado de direito privado*. 1st ed. BOOKSELLER.

[167] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[168] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[169] Warren, S. D. and Brandeis, L. D. (1890) "The right to privacy," *Harvard law review*, 4(5), p. 193. doi: 10.2307/1321160.

Constitution "conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men".[170]

To this aspect of privacy, the paradigm to be followed was the absence of communication between a person and others, taking the right marked by exacerbated individualism.[171] Therefore, except for rare exceptions[172], the right to personal data protection has not yet been recognized by federal legislation in the United States of America, resulting in the guidance that "Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information can generally be freely transmitted".[173]

Despite these facts, Daniel J. Solove recalls that the U.S. Supreme Court expounded an important conceptualization for privacy in the case Planned Parenthood v. Casey, in which it was indicated that the most intimate and personal choices a person can make throughout life, namely, choices centered on personal dignity and autonomy, are central to freedom, protected by the Fourteenth Amendment.[174]

Another important decision of the American Supreme Court occurred in 1967[175] when it was decided that once a person exposes their personal data to third parties, such as banks or other services, the latter do not have a reasonable expectation of privacy regarding government access. The following year, Alan Westin characterized privacy as the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others.[176]

---

[170] *OLMSTEAD et al. v. UNITED STATES. GREEN et al. v. SAME McINNIS v. SAME* (no date) *LII / Legal Information Institute*. Available at: https://www.law.cornell.edu/supremecourt/text/277/438 (Accessed: February 19, 2024).

[171] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[172] Among them, it is noteworthy to mention the FCRA (Fair Credit Reporting Act), aimed at regulating the privacy of consumer information.

[173] *U.S. West, Inc. v. Federal Communications Commission* (1999) *UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUITS*. Available at: https://cite.case.law/f3d/182/1224/ (Accessed: February 19, 2024).

[174] Solove, D. J. (2009) *Understanding Privacy*. London, England: Harvard University Press.

[175] *Katz v. United States, 389 U.s. 347 (1967)* (no date) *Justia Law*. Available at: https://supreme.justia.com/cases/federal/us/389/347 (Accessed: February 19, 2024).

[176] Westin, A. F. (1970) *Privacy and Freedom*. London, England: Bodley Head.

In this sense, all classes were subject to having their privacy infringed or affected by entities and institutions. The theorist Robert Post argued that privacy is not just a set of restrictions on society's rules and norms. Instead, privacy constitutes an attempt by society to promote civility.[177]

Note that privacy is not simply a way to free individuals from social control; it is itself a form of social control that emerges from society.[178] Therefore, privacy has social value; it is not simply an external restriction on society but rather an internal dimension of society. When the law protects the individual, it does so not only for the individual's sake but for the sake of society.

Emergence of Informational Self-Determination

Gerrit Hornung and Christoph Schnabel state that the idea of protecting personal data was introduced in the ruling of the well-known case of the German Census Act of 1983[179], which involved an attempt to census the population. The purpose of the collection was: a) to gather statistical information, such as population growth, demographic density, and economic activities, among others; b) to compare them with data stored in public records; and c) to send them, when necessary, to public authorities.

The German Constitutional Court declared the nullity of the legal provisions that provided for the comparison and transmission of the collected data to public authorities and recognized the existence of a right to informational self-determination, understood as the right of the individual to protect themselves against the collection, storage, use, and disclosure of their personal data, carried out unlimitedly, a right that could only be restricted in case of a public interest, based on constitutional grounds.[180]

It is worth remembering that in 1977, the Federal Republic of Germany created its first law on informational self-determination, which had the specific purpose of protecting individuals against

---

[177] Post, R. C. (2001) *Three concepts of privacy*, *Yale.edu*. Available at: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/1114/Three_Concepts_of_Privacy.pdf?sequence=2&isAllowed=y (Accessed: February 19, 2024).

[178] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[179] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[180] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

interference in the use of their personal data, a norm directed exclusively against state action that would negatively interfere (through unauthorized individual data collection) or positively interfere (preventing individuals from using the data as they please) in the individual self-determination of personal data.[181] The fundamental assumption of such legislative creation was the existence of an asymmetrical power and knowledge relationship between the data collecting entity (the State) and the subjects subjected to the data collection activity (private individuals, holders of the fundamental right).[182]

This legislation had two assumptions. First, with the establishment of the welfare state and the consequent increase in state functions, the collection of personal data became necessary for the organization of public functions, especially for the provision of public services efficiently and promptly.[183] Data collection, in this sense, was conceived as a means of protecting the user of public services, who has the right to continuity and quality of the public activity provided by the State or by concessionaires of these services.[184]

Second, for the realization of such activities, public bodies began to create large databases, in which information related to personal characteristics and habits began to be cataloged in a centralized and systematic manner.[185] The control power resulting from this accumulation of information was the trigger for the creation of a shield of protection of personal freedom.[186]

Without the guarantee that their actions would not be influenced by holders of personal information and that access to essential services would not be limited based on personal information, individual freedom and spontaneity would be chilled by the individuals themselves, who would control their actions by foreseeing possible damages that could result from them.[187] The protection of

---

[181] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[182] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[183] Buchner, B. (2020) *Informationelle Selbstbestimmung im Privatrecht*. JCB Mohr (Paul Siebeck). doi: 10.1628/978-3-16-158031-4.

[184] Dimoulis, L. M. D. (2020) *Teoria Geral Dos Direitos Fundamentais*. Nova Edição[a]. Revista dos Tribunais.

[185] Vesting, T. (2003) *Das Internet und die Notwendigkeit der Transformation des Datenschutzes*.

[186] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[187] Bull, H. P. (2013) *Netzpolitik: Freiheit und Rechtsschutz im Internet*. 1st ed. Baden-Baden, Germany: Nomos.

personal data thus emerges as a doubly instrumental right: not only does it protect individual freedom against unauthorized and excessive intrusions by the State - as is the case with all other fundamental rights, but it also ensures that all other fundamental rights are exercisable.

Such as freedom of expression, artistic freedom, freedom of movement, and freedom of assembly, are exercised and realized without the holders of these rights feeling threatened by an omnipresent and omniscient observer: the State.[188] Therefore, defending the protection of personal data was seen as synonymous with defending democracy and, conversely, those who opposed this right were identified as supporters of authoritarianism.[189]

This construction of apocalyptic and antigovernmental ideas took on dramatic political and social contours in the context of the trial of the constitutionality of the 1983[190] census law. Amid protests against the arms policy of the early 1980s, the slogan arose: "Down with the census."[191] It was the same State that harmed the environment, concentrated wealth, aligned itself with the combat policy established by the North Atlantic Treaty Organization, which now, surreptitiously, demanded that citizens provide data.[192] And if it, the State, is capable of carrying out such atrocious actions, what will it do with the data collected from the population?

It was for all these reasons that the census law concentrated the anger and fury of an entire generation formed by the constant and present threat of socialism and nuclear war: the threat of sudden destruction, caused by an enemy that is not even known.[193] Encouraged by state governments opposed to the expansion of federal power, more than four hundred protests were held against the census law, many of which called for a widespread popular uprising and even civil insurrection against the census law.[194] The response of the German Constitutional Court to this situation of

---

188 Britz, G. (2010) *Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts*.

189 Vesting, T. (2003) *Das Internet und die Notwendigkeit der Transformation des Datenschutzes*.

190 Simitis, S. (2000) *Das Volkszählungsurteil Oder Der Lange Weg Zur Informationsaskese*.

191 Buchner, B. (2020) *Informationelle Selbstbestimmung im Privatrecht*. JCB Mohr (Paul Siebeck). doi: 10.1628/978-3-16-158031-4.

192 Hoffmann-Riem, W. (1998) *Informationelle Selbstbestimmung in der Informationsgesellschaft*.

193 Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

194 Hoffmann-Riem, W. (1998) *Informationelle Selbstbestimmung in der Informationsgesellschaft*.

widespread social turmoil was simply the creation of the "Magna Carta of Personal Data Protection": a decision that states that there is no data without legal value since, after all, no matter how small the personal information is, when aggregated with other data, it can be the basis for the creation of informational profiles that replace concrete individuality.[195]

Another landmark decision in the evolution of the position on this right and its horizontal effectiveness concerning private life refers to decision BVerfGE 84, 192, of the year 1991. In the case, there was the signing of a lease contract with a person who had been legally incapacitated - partially - since 1963, due to "mental deficiency." At first, this factor was not disclosed, and there was an addendum signed by this person's guardian. Due to the lack of information provided, the lessors requested the termination of the contract. After going through the ordinary instances, the case was deliberated by the Constitutional Court. In this sense, the Court ruled that there was no general incapacity, but only partial, and that the lease obligations by this person were duly fulfilled. Therefore, and in the face of a stigmatizing disease, there would be no reasoned justification for the necessary disclosure of their legal incapacity, even more so "if the claimant had to disclose their legal incapacity without examining the question of whether their contractual opponent has a protected interest (...) it would be almost impossible for them to rent a space."[196]

This second decision brings two important points to the discussion on informational self-determination. First, it states that there is effectiveness of the right in the context of relations between individuals (horizontal effectiveness) since its application to an eminently private dispute was possible. Second, it refers to this as the instrument capable of protecting the individual from apparent or fictitious consent due to power imbalances with the other party, thus reaffirming its scope alongside the right to personality. Thus, we result in specific judicial control over contracts that regulate the processing of personal data.

For this reason, every data subject now has the right to know "who, where, how, and for what purpose their data has been used." Only in this way can individuals have the possibility of knowing who holds their data, which aspects of their personality have been identified and collected, and, finally, why the State and private entities have become interested in their lives and what purpose is sought by the collection of this personal data.

---

[195] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[196] Axel Tschentscher, L. L. M. (1991) BVerfGE 84, 192 - Offenbarung der Entmündigung, Unibe.ch. Available at: https://www.servat.unibe.ch/dfr/bv084192.html (Accessed: February 19, 2024).

At first glance, there are problems in this construction, starting with the assumption that people's personality can somehow be developed in a completely aseptic environment, without social interaction and without the daily transfer of data that arises from social contact and communication.[197] Therefore, society and the State cannot be expected to provide what they cannot offer: complete transparency regarding the use and destination of all data collected daily from all citizens of a country. After all, just as it is not possible to determine in advance whether information is true or false, it is not possible to foresee completely and determinedly what personal data will be used for.

This would simply mean the extinction of any possibility of implementing public policies and the consequent extinction of essential public services for the population.[198] Therefore, American jurisprudence until today considers the right to data protection to have a very limited character, as "even though we may feel uncomfortable knowing that our personal information circulates the world, the fact is that we live in a free and open society, where information must flow freely."[199]

This is exactly why legislation has focused on identifying the due informational process, that is, as we can see in the personal data protection law, there is express authorization for the shared use of data for the execution of public policies, demanding shortly thereafter, however, that the cases be informed in which, in the exercise of their competences, they carry out the processing of personal data, providing clear and updated information about the legal provision, the purpose, the procedures, and the practices used for the execution of these activities, in easily accessible vehicles, preferably on their websites.

From this point of view, it is verified that for the state act, it is necessary to comply with the principle of purpose and the linked administrative act, requiring legal authorization, for the provision of updated and efficient public services.[200]

---

[197] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[198] *U.S. West, Inc. v. Federal Communications Commission* (1999) *UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUITS*. Available at: https://cite.case.law/f3d/182/1224/ (Accessed: February 19, 2024).

[199] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[200] Hornung, G. and Schnabel, C. (2009) "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention," *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

In the Census decision, it was said as precisely as mysteriously, that every citizen has the right to "know who, how, when, and by what means their personal information reaches the knowledge of third parties."[201] This conclusion has two normative foundations - articles 1 (dignity) and 2 (freedom in a general sense), both of the Basic Law of Bonn - which, when combined, lead, in the understanding of the Court, to the conclusion that people have the right to develop their personality fully and without constraints imposed by the State or by society; and also a factual foundation that lies in the sudden development of automated databases, capable of mapping in detail all aspects of individual behavior.[202]

Combined with the constant fear of state political persecution and popular dissatisfaction with German foreign and energy policy[203], these foundations led to the creation of this new fundamental right: informational self-determination.[204]

This right provides the basis for contemporary general personal data protection codes. The preventive and accessory nature of the right to informational self-determination can help to contribute to a better understanding of transatlantic differences in personal data protection standards.[205]

A systematic preemptive right to personal data protection, which provides protection against mere potential harm, does not easily fit into this legal tradition. As Navarro defines: "Data are personal and their protection ensures the self-determination of personality."[206] The informational self-determination of the individual requires active participation from the data subject and, consequently, greater control over the flow of their personal information, constituting an active right and necessary participation of the individual in relation to its terms.

---

[201] Martins, L. (2005) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*.

[202] Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[203] Honnige, C., Kneip, S. and Lorenz, A. (eds.) (2011) Verfassungswandel Im Mehrebenensystem. 2011th ed. Wiesbaden, Germany.

[204] Hornung, G. and Schnabel, C. (2009) “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention,” *Computer law and security report*, 25(2), pp. 115–122. doi: 10.1016/j.clsr.2009.02.008.

[205] Isaak, J. and Hanna, M. J. (2018) “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,” Computer, 51(8), pp. 56–59.

[206] Ana Maria Neves de Paiva. O direito fundamental à autodeterminação informativa (2012).

On a macro level, in order to develop more regulations and mechanisms for governing personal data and to avoid their misuse, it is necessary to develop a clearer view of the fundamental issue of personal data ownership; that is, to whom the data belong and which aspects of that ownership can be waived or contracted under what circumstances and which aspects can never be contractually waived.

It is worth noting that the German Federal Constitutional Court continues to defend this right to this day. In February 2023, the Court issued a decision considering that §25a(1) of the Public Security and Order Act for the Hesse region (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung – HSOG) and §49(1) of the Police Data Processing Act for the Hamburg region (Hamburgisches Gesetz über die Datenverarbeitung der Polizei – HmbPolDVG) are unconstitutional. These provisions authorized the police to process personal data stored through automated data analysis (Hesse) or automated data interpretation (Hamburg). The provisions violate the general right to personality (Art. 2(1) together with Art. 1(1) of the Basic Law (Grundgesetz – GG) in its manifestation as the right to informational self-determination because they do not contain sufficient thresholds for interference. According to the Court, these laws allow for the subsequent processing of stored data through automated data analysis or interpretation in certain cases, subject to case-by-case evaluation, when necessary, as a precautionary measure to prevent specific criminal acts. Given the particularly broad wording of the powers, in terms of data and methods in question, the grounds for interference fall far short of the constitutionally required threshold of identifiable danger.[207]

These decisions by the German Federal Constitutional Court align with the European framework of fundamental rights protection, including both the European Union (EU) and the European Convention on Human Rights (ECHR). Firstly, they reflect the principles enshrined in the Charter of Fundamental Rights of the European Union, particularly concerning the right to privacy and data protection (articles 7 and 8). The Court's rulings emphasize the importance of safeguarding individuals' rights to informational self-determination and protecting personal data against unjustified interference by state authorities. Secondly, these decisions resonate with the jurisprudence of the European Court of Human Rights (ECtHR) regarding the right to privacy under Article 8 of the European Convention on Human Rights. The ECtHR has consistently emphasized the need for

---

[207] Bundesverfassungsgericht, 1. Senat (2023) Bundesverfassungsgericht - Entscheidungen - Regelungen in Hessen und Hamburg zur automatisierten Datenanalyse für die vorbeugende Bekämpfung von Straftaten sind verfassungswidrig, Bundesverfassungsgericht. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html;jsessionid=4C277453C112811049FBC9244433D0C5.1_cid507 (Accessed: February 19, 2024).

any interference with privacy rights to be proportionate, necessary, and subject to adequate safeguards.[208] Consequently, the European Court of Human Rights (ECtHR) has consistently demanded that the interception of communications be authorized by a law that is particularly precise. As elucidated by the Court, clear and detailed regulations are indispensable, especially given the continuous advancement of technology in this field. Specifically, domestic legislation must provide citizens with sufficient clarity regarding the circumstances and conditions under which public authorities are permitted to employ such measures.[209]

In this context, the German Constitutional Court's rulings underscore the significance of establishing clear legal thresholds for state interference with personal data, in line with the principles of proportionality and necessity. They highlight the importance of ensuring robust safeguards against arbitrary or excessive intrusion into individuals' privacy rights, thus contributing to the broader European framework of fundamental rights protection.

To this extent, the German court continues to indicate that legal provisions must indicate the grounds for interference in a proportional manner in light of the seriousness of the interference and the provisions, always based on respect for the right to informational self-determination.[210] We emphasize that this is a decision not only of individual but also of collective scope.

This will be important to contain current practices of companies that determine, through non-negotiable terms, that they can do whatever they please with users' personal data. It remains crucial that, with all technological promises innovations worth for a greater good, we do not lose sight of the ethical principles that keep us human. In general, humanitarian and development communities need to adopt a more rigorous and transparent approach to data protection and innovation.

---

[208] For example, in the case of *Kruslin v France* (1985), it was underscored that actions such as tapping and intercepting telephone conversations constitute significant intrusions into private life and correspondence. (Case of Kruslin v. France. Application no. 11801/85. Judgment 24 April 1999).

[209] 1) Case of Zakharov v. Russia. Application no. 47143/06. Judgment 4 December 2015; 2) Case of Iordachi and Others v. Moldova. Application no. 25198/02. Judgment 10 February 2009; 3) Case of Podchasov v. Russia. Application no. 33696/19. Judgment 13 february 2024; 4) Case of Nejdet Şahin and Perihan Şahin v Turkey. Application no. 13279/05. Judgment 20 October 2011; 5) Case of Rekvényi v Hungary. Application no. 25390/94. Judgment 20 May 19999; 6) Case of Hashman and Harrup v UK. Applicattion no 25594/94. Judgment 25 November 1999.

[210] Bundesverfassungsgericht, 1. Senat (2023) *Bundesverfassungsgericht - Entscheidungen - Regelungen in Hessen und Hamburg zur automatisierten Datenanalyse für die vorbeugende Bekämpfung von Straftaten sind verfassungswidrig*, *Bundesverfassungsgericht*. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html;jsessionid=4C277453C112811049FBC9244433D0C5.1_cid507 (Accessed: February 19, 2024).

2. **Regulatory Landscape in the United States of America**

The right to personal data protection refers to the legal framework that regulates the collection, use, and storage of personal information. It is designed to protect individuals from having their personal information misused or manipulated. It is based on the principle that individuals have control over their personal information and that organizations have a responsibility to handle it responsibly.[211]

There appear to be two types of personal data protection regulatory systems existing in various countries.[212] There is the comprehensive personal data protection system, which is broad and general ("omnibus"), with the action of a central and uniform authority, with concern for the regime in general. On the other hand, the second system is restricted and limited ("sectional"), opting for the absence of a global regimen but focusing on specific areas and according to the sensitivity of that area and its actors, both private and public. In most cases, there is no general authority for control.

In particular, it is noted that the choice of the omnibus system emphasizes the following principles: (1) limits on data collection, also called data minimization; (2) data quality principle; and (3) notification, access, and correction rights for the individual. In the system chosen by the United States of America, however, there has been a reinforcement of the concept of notification of data processing practices and consent of the affected party for processing. Certain principles, only recently being incorporated into specific legislation - and more forcefully into state legislation - which are already present in countries that adopt omnibus systems, such as (4) personal data processing carried out according to a legal basis; (5) regulatory supervision by an independent data protection authority; (6) enforcement mechanisms, including restrictions on exporting data to countries lacking sufficient privacy protection; (7) limits on automated decision-making; and (8) additional protection for sensitive data.

In the case of the United States of America, the right to personal data protection is governed by a combination of federal and state laws, as well as specific sectoral regulations, with no single

---

[211] Lynskey, O. (2014) Deconstructing data protection: the “added-value” of a right to data protection in the EU legal order. International and Comparative Law.

[212] Newman, A. P. (2008) Protectors of Privacy: Regulating Personal Data in the Global Economy.

authority with enforcement and control power, but with several bodies responsible, each in its specific category.[213]

Driven by the consumer protection movement, Congress passed the Fair Credit Reporting Act (FCRA) in 1970, which provides a set of basic rights guaranteed to citizens of that country (examples of rights include: right to information about credit report, right to obtain credit score for free, right to dispute incomplete and inaccurate information, right to consent to the transmission of information to potential employers). Furthermore, the Privacy Act can be indicated as the discipline on personal data protection, especially and solely focused on the use and sharing of personal data by federal government agencies of the United States. The S. 3418, commonly referred to as the "1974 Privacy Act," was enacted on December 31, 1974. This law is characterized as a comprehensive code of fair information practices that seeks to regulate the collection, maintenance, use, and dissemination of personal information by agencies of the Federal Executive Branch.[214]

Moreover, in the idea of sectoral regulation, in 1974[215], the "U.S. Privacy Protection Study Commission" was designated, which delved into the question of applying regulations to the private sector.[216] It is also noted that at the federal level, in 1996, the Personal Data Protection Act with a special focus on the health sector was promulgated, namely the Health Insurance Portability and Accountability Act (HIPAA), which applies to healthcare providers and organizations.[217] The Federal Trade Commission (FTC) also has the authority to regulate personal data protection and enforce laws against unfair or deceptive practices.[218] The Children's Online Privacy Protection Act (COPPA) is a

---

213 Guidi, G. (2017) Modelos regulatórios para proteção de dados pessoais. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio.

214 Waller, S. (2011) “Consumer protection in the United States: an overview. European Journal of Consumer Law, rotection in the United States: an overview,” European Journal of Consumer Law.

215 UNITED STATES. CONGRESS. SENATE. COMMITTEE ON GOVERNMENT OPERATIONS (1974) Legislative history of the Privacy Act of 1974, S. 3418 (Public Law 93-579) source book on privacy, https://tile.loc.gov/storage-services/service/ll/llmlp/lh_privacy_act-1974/lh_privacy_act-1974.pdf. Available at: https://tile.loc.gov/storage-services/service/ll/llmlp/LH_privacy_act-1974/LH_privacy_act-1974.pdf (Accessed: February 19, 2024).

216 Solove, D. J. and Hartzog, W. (2014) “The FTC and the New Common Law of Privacy,” Columbia Law Review, 114, pp. 583–676.

217 UNITED STATES. (1977) Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission transmitted to President Jimmy Carter, https://epic.org/privacy/ppsc1977report/c1.htm. Available at: https://epic.org/privacy/ppsc1977report/c1.htm (Accessed: February 19, 2024).

218 *Health insurance portability and accountability act of 1996 (HIPAA)* (2022) *Cdc.gov*. Available at: https://www.cdc.gov/phlp/publications/topic/hipaa.html (Accessed: February 19, 2024).

federal law that applies to websites and online services that collect personal data from children under 13 years of age.[219]

At the state level, 13 (thirteen) states have already passed specific laws on the subject. The states of California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia have their own legislation to regulate aspects of personal data protection, at least in the consumer field.

Basically, the right to personal data protection in the United States is governed by a combination of federal and state laws, especially regarding consumer protection. These laws grant individuals the right to know what personal data is being collected about them, request its deletion, and opt-out of the sale of their personal data. They also impose obligations on organizations to handle personal data responsibly and ethically.[220]

Furthermore, in the regulatory field, the Federal Trade Commission (FTC) is a United States government agency whose primary function is antitrust law enforcement (non-criminal) and promotion of consumer protection, being one of the most active agencies in regulating and enforcing regulations on the subject. The FTC itself has drafted a report with guidelines for companies and data subjects, and its guidelines are for processing to follow 3 (three) core principles[221]: (i) Privacy by Design; (ii) Simplified Consumer Choice, and; (iii) Transparency.

An example of a legal case involving personal data protection that was decided by the Supreme Court of the United States is Carpenter v. United States (2018).[222] In this case, the defendant, Timothy Carpenter, was convicted of several robberies. The government used his cellphone location data, obtained from his cellphone carrier without a warrant, as evidence against him. The defendant argued that the warrantless collection of his cellphone location data violated his rights under the Fourth Amendment against unreasonable searches and seizures.[223]

---

219 Solove, D. J. and Schwartz, P. M. (2023) *Information privacy law*. 8th ed. Aspen Publishing.

220 Solove, D. J. and Schwartz, P. M. (2023) *Information privacy law*. 8th ed. Aspen Publishing.

221 *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers* (2012) *Federal Trade Commission*. Available at: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (Accessed: February 19, 2024).

222 Tokson, M. (2018) "The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021," *Havard Law Review*, 135, pp. 1791–1851.

223 U.S. SUPREME COURT (2017) *Carpenter v. United States*, *Supremecourt.gov*. Available at: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (Accessed: February 19, 2024).

The Supreme Court ruled in favor of Carpenter, holding that the warrantless collection of his cellphone location data was a violation of his rights under the Fourth Amendment.[224] The Court stated that geolocation data involves a "comprehensive chronicle of a person's physical presence compiled every day, every moment, over several years."[225] The Court's decision is significant because it recognizes that individuals have a reasonable expectation of privacy in the location data of their cellphones and that this information is protected by the Fourth Amendment of the country. This case highlights the importance of data protection rights and the need for the government to obtain a warrant before collecting personal information to respect individuals' privacy rights.

Finally, it is worth noting that the United States of America currently has a valid legal basis for data transfer by the European Union after long controversy. Let's go through the history. In 2016, the European Union adopted an adequacy decision called the EU-US Privacy Shield, which allowed the transfer of personal data from the European Union to that country. In this multilateral agreement, the United States Department of Commerce and the European Commission established a set of principles and safeguards to be guaranteed by companies adhering to the agreement to enable the transfer of personal data of individuals located in the European Union to companies located in the United States.[226] However, in the case known as Schrems II, the Court of Justice of the European Union declared this instrument null and void, as the adequacy of the Privacy Shield as a valid legal basis for international data transfer was not recognized.

The Court's decision to invalidate the EU-US Privacy Shield was directly tied to the fundamental right to protection of personal data guaranteed by the European Union. This right is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU), which safeguards individuals' privacy and data protection. Additionally, Article 16, § 1 of the Treaty on the Functioning of the European Union (TFEU) reinforces the importance of protecting personal data within the EU legal framework. In the Court's view, the surveillance programs implemented by the United States government were deemed to disproportionately violate individuals' privacy and data protection rights as guaranteed by the GDPR. This disproportionate violation of fundamental rights,

---

224 Kerr, O. S. (no date) “An Equilibrium-Adjustment Theory of the Fourth Amendment,” *Havard Law Review*, 125.

225 Kerr, O. S. (no date) “An Equilibrium-Adjustment Theory of the Fourth Amendment,” *Havard Law Review*, 125.

226 *Implementing decision - 2016/1250 - EN - EUR-Lex* (no date) *Europa.eu*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG (Accessed: February 19, 2024).

as understood by the Court, necessitated the invalidation of the Privacy Shield agreement, which was intended to facilitate international data transfers while ensuring adequate protection of personal data.

This ruling underscored the fundamental importance of the principle of proportionality in European Union law, particularly within the realm of safeguarding fundamental rights as enshrined in Article 52, § 1 of the Charter of Fundamental Rights of the European Union. Throughout various rulings, the Court has consistently emphasized the significance of reasonableness (proportionality) in the measures implemented, always with the aim of ensuring the protection of rights delineated in the Charter.[227] This principle requires that any action taken by public authorities, including those related to data protection and privacy, be proportionate to the intended objective and not exceed what is necessary to achieve that goal. In the context of international data transfers, the Court's application of the proportionality principle reflects its commitment to upholding the rights and values enshrined in EU law while addressing the complex challenges posed by global data governance and surveillance practices.

In effect, by not clearly foreseeing the limitations of the powers granted to intelligence services, the surveillance programs end up allowing public authorities to carry out excesses, which are not limited to what is strictly necessary to ensure national security, as provided for in the GDPR. However, it's important to note that the CJEU did uphold the validity of the European Commission's standard contractual clauses for data transfers to the USA in the same ruling. This decision was significant as it provided a clear pathway for organizations to continue conducting cross-border data transfers while ensuring compliance with the GDPR's stringent data protection standards. By validating the SCCs, the CJEU acknowledged their role as a robust legal mechanism for safeguarding personal data when transferred to third countries. The CJEU's decision regarding the SCCs underscored their importance as a flexible and adaptable tool for facilitating international data transfers, offering organizations a viable alternative to the now-defunct Privacy Shield framework.

---

[227] 1) Case C-301/06. Ireland v. European Parliament and Council of the European Union. Judgment 10 February 2009; 2) Case C-293/12 and C-594/12. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e others. Judgment 08 April 2014; 3) Case C-207/16. Ministério Fiscal. Judgment 02 October 2018; 4) Case C398/15. Câmara de Comércio, Indústria, Artigianato and Agricoltura di Lecce v. Salvatore Manni. Relator M. Ilešič. Judgment 09 March 2017; 5) Case C-136/17. GC e outros v. Commission nationale de l'informatique et des libertés (CNIL). Judgment 24 September 2019; 6) Case C-360/10. Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV. Judgment 16 February 2012; 7) Case C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Judgment 29 January 2008.

This validation provided much-needed reassurance to businesses and individuals alike, offering a practical solution to the complex challenges posed by global data flows in the digital age.

In this regard, the European Commission initiated a new process to adopt a decision of adequacy of the EU-US Data Privacy Framework, called the Adequacy Decision for the EU-US Data Privacy Framework, which sought to foster transatlantic data flows and address the concerns raised by the Court of Justice of the European Union in the above decision, which was approved by the European Commission in 2023.

The European Commission approved the request after the publication of Executive Order No. 14086 by the Federal Government of the United States of America and supplemented by the Regulation approved by the Department of Justice of that country ("EO 14086" and "AG Regulation").

As provided in the Executive Order and the Department of Justice Regulation, the Data Protection Review Court will be created, which will be the Independent Authority, with powers of binding decision on the Federal Government, to which individuals from the European Union may submit complaints, free of charge, to the so-called Civil Liberties Protection Officer of the US Intelligence Community, and, in the second instance, individuals will have the right to appeal the decision to the newly created Data Protection Review Court.

The Court (or Authority) will be composed of members chosen by individuals not affiliated with the government of the United States of America, appointed based on their previous qualifications and who can only be dismissed for serious misconduct and cannot receive instructions from the Government for making their decisions. Thus, the Court (or Authority) will have powers to investigate complaints from Union individuals, including obtaining information from intelligence agencies of the United States of America and may adopt binding corrective decisions.

Following this, companies based in the United States of America will be able to self-certify their entry into the EU-US Data Privacy Framework, committing to comply with a detailed set of privacy obligations, such as deleting personal data when it is no longer necessary for the purpose for which it was collected and ensuring the continuity of protection, in accordance with the terms of Executive Order No. 14086.

Finally, it is worth noting that the European Union already had an Adequacy Decision with the United States of America, regarding the protection of personal information related to the prevention, investigation, detection, and repression of crimes. Decision 2016/920 is dated 2016 and

aims to establish principles and guarantees regarding the protection of personal data transferred for the purpose of criminal law enforcement between the United States, on the one hand, and the European Union and its Member States, on the other. The objective is to ensure a high level of protection of this data and, thus, enhance cooperation between the Parties. Although not constituting the legal basis for the transfer of personal data to the United States, the agreement complements, when necessary, the guarantees regarding data protection provided for in existing or future agreements, concerning data transfer or in national provisions authorizing such transfers.

3. **Subjective and Objective Dimensions of the Right to Personal Data Protection**

Fundamental rights generally have a dual dimension, namely the subjective and objective.[228] In its subjective condition, the right to personal data protection can be understood as a set of heterogeneous and subjective defensive positions (negative), but it also assumes the condition of a right to provisions, whose object consists of the principle of accountability and accountability. That is, when referring to the subjective dimension of the right, one will be faced with the rights attributed to that right, its effective application in the life of each human being. And in the present case, as already specified in the above topic, the rights attributed to the data subject are the subjective legal positions of this right being studied here. Thus, the aim is to elucidate and clarify the realization, thus ensuring the double function of such a right as a negative (defense) and positive (provisional) right.

Regarding the objective dimension, we must evaluate the three instances of this dimension, namely, (i) effectiveness; (ii) protection duties; (iii) procedures to guarantee and enforce the right.[229]

Regarding the topic of effectiveness, it must be observed that the protection of personal data is of special interest in caring for the human being in the face of private actors, since it is these actors

---

[228] Sarlet, I. (2018). *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado*.

[229] Regarding the objective dimension, Ingo Sarlet stated: "the paradigmatic assertion of the Federal Constitutional Court is always recalled, according to which fundamental rights are not limited to the primary function of being subjective rights for the defense of the individual against acts of public authority, but also constitute evaluative decisions of a juridical-objective nature of the Constitution, with effectiveness throughout the legal system, providing guidelines for legislative, judicial, and executive bodies. However, it is also worth recalling that the objective perspective of fundamental rights does not represent a mere 'flip side' of the subjective perspective, but rather means that autonomous function is granted to norms that provide subjective rights, which transcends this subjective perspective and, moreover, leads to the recognition of normative contents and, therefore, distinct functions for fundamental rights." (Sarlet, I. (2018). *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado*).

who produce content – especially on the World Wide Web – capable of generating eventual restrictions/ injuries to this right. Thus, there must be control over restrictions on fundamental rights in the sphere of private relations, including preventively, considering especially the legislative options of that nation.

Regarding the second topic, protection duties, these are especially focused on the protection that the State must safeguard, including preventively, not only against the Public Power (internal and external) but also against attacks by individuals. In relation to the right to the protection of personal data, we can identify that the edition of state legislation and its system of material and procedural guarantees was the main protective milestone of the protection duties.

Regarding the third item, procedures to guarantee and enforce the right, it is already identified that the above item brings the state regularization of its protection and effectiveness attempt. However, delving into the topic at hand here, we can see that the principle of data protection from the conception of processing systems ("privacy by design") to the creation of means to contain defects in operations ("privacy by default") are the final definers of this topic, as practical ways of executing and processing personal data safely and reasonably by third parties.[230]

In this way, the creation of the two dimensions of the right to the protection of personal data is verified, with its foundation to reinforce the legal regime and translate the right, especially focused as a fundamental guarantee.

Furthermore, defining the protection of personal data as a fundamental right and having a rule system to regulate it leads to postulating what may be the essence of this right to personal data protection, being certain that this topic seeks to elaborate the vision on the essence of the right to personal data protection.[231] Understanding the essence, at least in our view, of a right has the advantage of better considering the specificities of each right and the legal and political context in which it was developed.[232] The distinction between the protection of personal data and substantive rights lies in their respective nuances and essential elements. While personal data protection focuses on safeguarding individuals' privacy and controlling the use of their data, substantive rights encompass a broader spectrum of rights, including intellectual property rights like copyright.

---

[230] Waldman, A. E. (2018). Privacy, notice, and design. *Stanford Technology Law Review*, *21*, 160–161.

[231] Lenaerts, K. (2019). Limits on Limitations: The Essence of Fundamental Rights in the EU. *German Law Journal*, *20*, 779–793.

[232] Dawson, M. E., & Orla E Muir, E. (2019). What is the Added Value of the Concept of the “Essence” of EU Fundamental Rights? *German Law Journal*, *20*, 763–778.

Copyright, as a form of intellectual property right, indeed presents complexities in its categorization. It intersects with the right to protection of personal data in various contexts, such as in the digital environment where data privacy and copyright considerations often overlap. However, it's important to note that copyright primarily pertains to the protection of creative works and expressions, rather than personal data specifically. Regarding its classification as a substantive right, copyright is typically considered as such due to its role in protecting the intellectual creations of individuals or entities. However, its precise categorization can vary depending on legal frameworks and interpretations within different jurisdictions.[233] In the context of EU law, the framework for copyright protection is indeed multifaceted and not entirely unified, which can complicate its relationship with the right to protection of personal data.[234] The intersection between these legal domains underscores the need for careful consideration and balanced approaches to address the complex challenges arising from technological advancements and evolving legal landscapes.).[235] If these attributes represented the essence of data protection, their comparison would not be allowed, which does not seem to be the case. In this sense, we can understand the protection of personal data as, at a systemic level, checks and balances in which they are embodied to express society's stance towards the processing of personal data by third parties.[236]

Thus, we will study the essence of the right to the protection of personal data to collaborate with the research and updating of this essential topic for legal studies. The essence of the protection of personal data is to safeguard the rights and freedoms of individuals with respect to the processing of their personal data. This includes protecting individuals from possible harms that may arise from the improper handling of their personal data, such as discrimination, identity theft, or reputational harm.

Laws and regulations for the protection of personal data establish a framework for the collection, storage, and use of personal data and establish specific rules and procedures that organizations and governments must follow to ensure that personal data are treated fairly and

---

233 HUGENHOLTZ, P. Bernt; VAN VELZE, Sam C. (2016) *Communication to a new public?* Three reasons why EU copyright law can do without a 'new public'. International Review of Intellectual Property and Competition. p. 797-816.

234 APLIN, Tanya. (2005) *Copyright law in the digital society*. Oxford: Hart.

235 PORCEDDA, Maria Grazia. **On Boundaries – Finding the Essence of the Right to the Protection of Personal Data.** *In* LEENES, Ronald. (org.) *Data Protection and Privacy – The Internet of Bodies.* Hart Publishing. PP. 277 – 312. 2018. P. 289.

236 Brkan, M. (2016). The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors? *Maastricht Journal of European and Comparative Law*, *23*(5).

securely, and respect individuals' privacy rights. This includes, among other things, requirements for organizations to obtain informed consent before collecting personal data, provide individuals with clear and concise information about how their personal data are being collected, used, and shared, and notify individuals and authorities in case of data breaches.

The protection of personal data also includes rights for individuals, such as the right to access, rectify, or erase their personal data and the right to object to the processing of their personal data. In this way, the essence of the protection of personal data is to ensure that personal data are treated responsibly, transparently, and legally and safeguard the rights and freedoms of individuals with respect to their personal data.

Robert Alexy, commenting on the theory of spheres developed by the German Constitutional Court, clarifies that there are three spheres of protection, with varying and decreasing intensities. (i) The sphere, said to be lower, protected absolutely, and by legislation, fully, comprising the most secret matters that should not be known to others due to their extremely reserved nature; (ii) The expanded private sphere, which consists of matters that the individual brings to the knowledge of another trusted person, excluding the rest of the community, which can be known by the individual himself or the community at large; (iii) The sphere of communication, with the least intensity, comprising matters that the individual brings to the knowledge of everyone, which can be known by the individual himself or by everyone in the community.[237]

With the current portrayal of the subject, Maja Brkan depicts possible interferences with fundamental rights as concentric circles, where, in the outermost layer, there is no interference with the right and then - progressing towards the center - justified interference, unjustified interference, serious interference, and interference with the essence of the right. The distinction between interferences is particularly significant in light of the debate surrounding the relationship between balancing (proportionality sensu lato) and the essence of fundamental rights.[238]

A relativizing stance admits the possibility of compressing the essence of a fundamental right to safeguard another fundamental right, an absolute stance constructs essence and proportionality as mutually exclusive concepts. To explain better, theorizing the essence of the right to personal data protection is significant regardless of adhering to an exclusive or integrative stance. In the first case,

---

[237] Alexy, R. (1997). *Teoria dos derechos fundamentales. Trad. Ernésto Garzón Valdés. Madrid: Centro de Estudios Constitucionales*.

[238] Brkan, M. (2016). The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors? *Maastricht Journal of European and Comparative Law*, *23*(5).

it identifies unacceptable interferences regardless of the relative nature of the right to data protection; in the second, it allows for mitigating the gradation of interference based on the realization or assessment of the balancing test.

In this sense, Takis Tridimas and Giulia Gentile argue that there are three ways to analyze the essence of a right. First, the essence can be seen as an inviolable core in which interference cannot be legitimately interfered with a limit whose compression cannot be justified by compelling/superior reasons. In this sense, the essence acts as an additional limit and identifies the type of interference with a right that cannot be legitimized by proportionality.[239]

Secondly, they continue to assert that the concept of essence can be seen, through the lens of a relative stance on interference itself, from the parameter of the most serious interference that one has on a right. It focuses, therefore, on the legal interest that the right seeks to protect and identifies the essence as the part of the right that is necessary to provide effective protection to that interest. In this conception, the essence is violated whenever the imposed limitations prevent its exercise and deprive it of any legal protection.

A third view of the essence is the limit beyond which an interference with the right leads to its extinction.

Returning to Brkan's teachings, the essence of a fundamental right suffers interference if (1) the interference threatens the very existence of that right, whether for all rights holders or for a specific right holder or group of rights holders; and (2) if there are no compelling reasons for such interference.

The principle that the essence of a right is violated when its existence is questioned without compelling reasons for restriction, thus introducing considerations of proportionality, finds illustration in various rulings of the Court of Justice of the European Union (CJEU). Here are some examples: In Case C-301/06, Ireland v. European Parliament and Council of the European Union (Judgment 10 February 2009), the legality of data retention laws and the balance between privacy rights and security interests were examined. Similarly, in Case C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung e.a. (Judgment 08 April 2014), the validity of EU data retention directives and their compliance with fundamental rights were at the forefront. In Case C-207/16, Ministério Fiscal (Judgment 02 October 2018), the proportionality of national legislation imposing tax penalties and

[239] The Essence of Rights: An Unreliable Boundary? (2019). *German Law Journal. PP*, *20*.

its impact on the right to property were discussed. Another case, C 398/15, Câmara de Comércio, Indústria, Artigianato and Agricoltura di Lecce v. Salvatore Manni (Judgment 09 March 2017), examined the compatibility of Italian legislation on immovable property auctions with EU law, focusing on the right to property. Furthermore, in Case C-136/17, GC and Others v. Commission nationale de l'informatique et des libertés (CNIL) (Judgment 24 September 2019), the balance between the right to privacy and the right to freedom of expression in the context of internet search engine delisting requests was deliberated. Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV (Judgment 16 February 2012), dealt with the balance between copyright protection and the rights of internet service providers regarding user-generated content. Lastly, Case C-275/06, Digital Promusicae v. Telefónica de España SAU (Judgment 29 January 2008), examined the balance between the right to copyright protection and the right to privacy in the context of disclosing internet user data for civil proceedings.[240]

Following such a structure and the framework of personal data protection described above, this topic argues that a violation of the essence of the right to personal data protection is a strong enough compression to threaten the very existence of the system of checks and balances on which the right to data protection is based, when there are no compelling reasons for doing so.

The first part of the test determines the presence of an interference in the essence of the right, which occurs when the very existence of the right is questioned for rights holders (objective interference in the essence) or for a specific rights holder (subjective interference in the essence). The second part of the test defends the exclusive position, which conceives interference with the essence of the right as unjustifiable by balancing and - conversely - does not consider interference with the right as compression of its essence in all cases where it can be justified, by reference to compelling reasons (i.e., balancing). Thus, Brkan's test to determine an interference in the essence of a fundamental right is particularly interesting considering the conception of the right to personal data protection outlined in this thesis.

Personal data protection is not an absolute right, so it can be legitimately compressed by other primordial rights; it can also be illegitimately usurped, which would result from the balancing test favoring personal data protection over the other conflicting right. In EU law, no fundamental right is considered absolute. Instead, each right must be balanced and articulated with other fundamental

---

[240] Dalla Corte, L. (2020). *Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment*.

rights using the principle of proportionality. This principle requires that any restriction or limitation on a fundamental right must be necessary and proportionate to achieving a legitimate aim. Therefore, in cases where personal data protection conflicts with other rights, such as freedom of expression or national security, a careful balancing exercise is required to ensure that the restrictions placed on personal data protection are justified and proportionate to the competing interests at stake.[241]

A violation of the essence of the right to personal data protection would exist, therefore, in cases where the interference with the right challenges, explicitly or implicitly, society's choice to have a legal framework for the processing of personal data. Think of all the ways in which the system of checks and balances on which personal data protection is based can be practically eradicated by neglecting, exploiting, or misinterpreting the provisions of derivative law that are not directly mentioned in art. 5th, LXXIX, of the CF/88 or defined as "fundamental" by the STF, such as perhaps the provisions on transfers of personal data to third countries or international organizations.

Limitations on the right to personal data protection should be the exception, not the rule. Thus, the essence of the system of checks and balances on which data protection is based - the "fundamental right to a rule" regulating the processing of personal data - should be seen as the collective decision to generally allow the processing of personal data because of its promises while at the same time regulating it because of its dangers. An interference with the essence of the right to personal data protection is therefore different from a regular interference, regardless of how serious. While the former harms part of the system of checks and balances of personal data protection, the latter questions and jeopardizes the very functioning and legitimacy of the collective stance on data processing as a whole and, ultimately, its deeper roots: the rule of law and democracy. Drawing a parallel with copyright in the EU legal order, where exceptions or limitations are strictly construed, underscores the gravity of interfering with the core principles of personal data protection. Just as exceptions to copyright are carefully circumscribed, limitations on the right to personal data protection should be approached with caution and reserved for truly exceptional circumstances.[242]A right to a permissive and procedural rule, allowing - and still channeling - an activity as fundamental to modern society as it is possibly dangerous. The *sui generis* emergence of personal data protection

---

[241] POLAKIEWICZ, Jörg. (2003) Profiling – the Council of Europe's Contribution. *In:* GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection:* coming of age. London: Springer, p. 367-377. p. 372.

[242] HUGENHOLTZ, P. Bernt; VAN VELZE, Sam C. (2016) *Communication to a new public?* Three reasons why EU copyright law can do without a 'new public'. International Review of Intellectual Property and Competition. p. 797-816.

is linked to technological development and its constitutionalization to the growing importance of secondary legislative framework. Lorenzo Dalla Corte brings the notion that the right to personal data protection has the idea of proceduralism, which he defines as "a theory that justifies rules, decisions, or institutions by reference to a valid process, as opposed to being morally correct according to a substantive account of justice or goodness."[243]

Given the heterogeneity of the rights and principles underlying the fundamental right, its formal (and practical) differentiation from privacy, and its procedural/instrumental and permissive nature, this thesis argues that the most coherent conceptualization of the right to personal data protection is of a system of rules and principles that regulate the processing of personal data by virtue of its potential impacts on individuals and society.

The essence of the right to personal data protection has been framed as the collective and social choice to have a system of checks and balances regulating the processing of personal data. The violation of the essence of the right to data protection can be defined as a compression strong enough to threaten the very existence of such a system of checks and balances when compelling reasons do not exist, regardless of which specific component of the right is compressed.[244]

Personal data protection is a non-homogeneous set of rules and norms whose content hardly fits into a unitary logic. Technological development, the spread of informatics, and the rampant datafication of society have led to the development of a sui generis right that no longer equates to privacy - if it ever did - but to something different, new, and still in flux, which was then elevated to the status of a fundamental right.

Personal data protection is a response to the power and information asymmetries that exist between those who control the means of data processing and the individuals to whom this data refers and responds to a recent need for protection that has emerged in parallel with advances in information technologies and their role in contemporary society.

In a way, the justification for the elevation of personal data protection to the status of a fundamental right should not be sought in the conceptual autonomy or systematic coherence of the heterogeneous array of rights and principles that constitute personal data protection. On the contrary,

---

[243] Dalla Corte, L. (20020. *Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment*.

[244] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile Books.

it is the constitutionalizing of personal data protection as an autonomous fundamental right that helps delineate its substance.

The seemingly inconsistent set of rights and principles underlying personal data protection, in the face of its explicit constitutionalizing by the Charter and assuming the democratic legitimacy of the underlying legislative process, creates a pragmatic system of protection that should be seen as the embodiment of such choice.

The conceptualization of the right to personal data protection serves the purpose of explicitly delineating how it expresses a defined social stance regarding the processing of personal data. More importantly, recognizing the conceptual autonomy of personal data protection and its links to the advancement of computing technology and thus modern society could promote the development of the right, to its full potential.

Procedural rights refer to the legal process and procedures that individuals and organizations must follow to have their rights protected and respected. These procedures aim to ensure fairness, impartiality, and transparency in legal proceedings and decision-making processes. Examples of procedural rights include the right to a fair trial, the right to be informed of the charges against you, the right to legal representation, the right to summon and examine witnesses, the right to appeal a decision, and the right to access court records.[245]

Procedural rights are important because they ensure that individuals and organizations are not subjected to arbitrary or discriminatory treatment by the state or other authorities. They also provide a means for individuals and organizations to challenge decisions that may negatively affect them and seek redress for any violations of their rights.

The most coherent construction of personal data protection is simply the fundamental right to have a set of rules regulating the processing of personal data. The value of personal data protection lies, in a way, in the existence of a system of rules and norms applicable to the processing of personal data, regardless of its connection to concepts such as privacy, or the secrecy and confidentiality of information.

The fundamental right to personal data protection has emerged therefore and response to the rampant digitization of society and the increasing importance of information (personal) processing. Its core, whose content depicts a heterogeneous range of rights and principles of personal data protection.

---

[245] Carnelutti, F. (1999). *Instituições do processo civil. Trad. Adrián Sotero de Witt Batista. Campinas: Servanda*.

A right to a rule, therefore, its logic is closer to due process than privacy. This dimension of the right may have already been observed since the early discussions about this normative innovation.[246] In 1973, in a study prepared for the United States Department of Health, Education, and Welfare, the main aspects and foundations for the proper processing of citizens' data, especially aimed at the three areas of that Department, were dissected.

This study elaborated in the 1970s serves as a basic parameter for understanding this right, and it is seen that the reasons for its study and presentation are paramount to understanding the growing concern about the harmful consequences that may result from the uncontrolled application of computer and telecommunications technology for the collection, storage, and use of personal data about citizens. In fact, the Secretary of Health, Education, and Welfare of the United States at the time of the study emphasized the public interest in establishing rules and principles for the care of personal data:

The study carries with it the primordial idea of transparency to the public regarding the treatment of personal data and its purpose, including its sources, its uses, and the justification for retaining it. Furthermore, the study records that it is based on five basic principles that would have legal effect as safeguard requirements for automated systems of personal data, namely:

> "- There should be no systems for maintaining records of personal data whose very existence is secret.
> - There must be a way for an individual to find out what information about him is in a record and how it is used.
> - There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
> - There must be a way for an individual to correct or alter a record of identifiable information about him.

[246] Docksey, C. (2015). *Articles 7 and 8 of the EU Charter: Two Distinct Fundamental Rights. in GROSJEAN, Alain (org.) Enjeux européens et mondiaux de la protection des données personelles*.

> - Any organization that creates, maintains, uses, or discloses records of identifiable personal data must ensure the reliability of the data for the intended use and must take precautions to prevent the misuse of the data."[247]

Moreover, the study itself delves into the need to protect identifiable or identified personal data of human beings, and with care to protect data, even if made available in anonymized form.

The essence of the system of checks and balances on which data protection is based—the "fundamental right to a rule" regulating the processing of personal data—should be seen as the collective decision to generally allow the processing of personal data because of its promises, while at the same time regulating it because of its dangers. An interference with the essence of the right to personal data protection is therefore ultimately an affront to the rule of law and the dignity of the human person. Substantive rights, on the other hand, refer to the actual rights and freedoms to which individuals and organizations are entitled under the law. These rights are designed to protect and safeguard the interests and well-being of individuals and organizations. Examples of substantive rights include the right to life, liberty, and security of the person; the right to freedom of expression, religion, and assembly; the right to property, the right to privacy, the right to education, and the right to fair and equal treatment under the law.

Substantive rights are important because they provide the basis for the ability of an individual or organization to live a full and meaningful life and to fully participate in society. They also provide an important check against the arbitrary or discriminatory use of power by the state or other authorities.

Thus, the role of substantive law is to confer legality on citizens, that is, to make them guarantors of positive legal norms for their protection. Pérez Luño refers to this idea of the dignity of the human person, as well as the demands and needs linked to the conquest of freedom and equality, from which human rights derive. These essential rights have a foundation that predates positive law, that is, preliminary and basic in relation to it. It is therefore clear that the reference to provisions on personal data protection stands out as a procedural system of heterogeneous checks and balances that gradually dissociates from the logic of privacy.[248]

---

[247] *Records, computers and the rights of citizens*. (n.d.). ASPE. Retrieved February 20, 2024, from https://aspe.hhs.gov/reports/records-computers-rights-citizens

[248] Luño, A.-E. (2005). *Derechos Humanos, Estado de Derecho y Constitución. 9*.

Conclusion

Thus, we can outline the main aspects of personal data protection as follows: the subject is any natural person, from that country or foreign, resident, or transient in that country or region. The content is the specific faculty attributed to the subject, which may be the faculty to deal with their data by others, or to resist them, or to dispose of, enjoy, or handle their personal information. Personal data protection, as a right, has as its content the faculty to constrain others to respect it and to resist the violation of what is proper to it, that is, the vital situations that, as they concern only the individual, they wish to keep for themselves, sheltered by their sole and discretionary decision. The object is the protected good, which may be *a res* (a thing, not necessarily physical, in the case of real rights) or an interest (in the case of personal rights). In the right to personal data protection, the object is, succinctly, informational self-determination.

The subject can be clearly verified in the legal text, since the legislator himself affirmed that the data subject is the person to whom the data refer and not the person who collected them. Moreover, protection must be limited to subjects with identifiable data or identified individuals. When data is disclosed, as an example, in statistical form, reasonable precautions must be considered, with the aim of fulfilling the obligation not to disclose data that can be traced back to specific individuals.

However, it is worth mentioning the existence of literature in an extensive sense, which guarantees legal entities a personal data protection equivalent to that of natural persons, which refers to the proposition that personal data protection has an instrumental nature, also serving (but not only and not necessarily) to safeguard privacy. In any case, even though we adhere to the position, for now, the legislation determines that the right to personal data protection is held only by natural persons. Furthermore, for the record, legal entities and even other entities can be holders of fundamental rights, compatible with their condition.

Still on this point, even though personal data protection as such is guaranteed only to natural persons, the same does not occur with the ownership of the right to informational self-determination, which, although also controversial, has been, at least in some legal orders — as is the case in Germany — equally attributed to legal entities.

We see that, through these two concepts, there is a great differentiation of object and objective. While the right to privacy seeks to defend the individual's intimacy and private (and family) life, the right to personal data protection is the protection of personal data itself, its use, its collection. Although it protects the individual, since it protects the individual from the search of third parties for collected and organized information that can describe, identify, qualify, and standardize such person and their life, this defense of the individual should be understood as a mediate objective.

Furthermore, it is reaffirmed that transparency about how personal data is processed is the key to the proper functioning of the market. Data subjects must know when and how their personal data is being collected and used and be able to decide whether and how to participate; and they must have access to companies' information on how they are collecting, storing, and using it, so they can select the company that best meets their preferences.

However, given the scale and complexity of personal data processing practices, it is argued that such transparency will not be sufficient to guarantee effective protection of personal data. It is suggested that the principle of controller/processor responsibility should play a more effective role in ensuring effective control over personal data. This accountability is a form of collective approach in that it strengthens the individual in relation to the controller/processor.

Indeed, individuals are recognized rights and protective instruments – such as the right to be forgotten, simplified access to data, the right to portability, and the right to know when data has been hacked. Data controllers and processors, on the other hand, are required to follow the principle of data protection from the design of processing systems ("privacy by design") to the creation of means to contain defects in operations ("privacy by default"). The object of the right to data protection is to protect personal data, which is any information that can be used to identify an individual, such as name, address, or biometric data. Personal data can be confidential, such as health information or information about an individual's political or religious opinions, or may not be confidential, such as information about an individual's name and address.

The right to data protection aims to ensure that personal data is collected, used, and stored in a way that respects individuals' privacy rights and that personal data is accurate, complete, and up to date. Data protection laws are designed to give individuals control over their personal data, including the right to access, correct, delete, and object to the use of their personal data for certain purposes.

The right to data protection also imposes obligations on organizations that collect and process personal data, such as obtaining explicit consent from individuals before collecting their personal

data, informing them about how the data will be used, and providing them with the ability to control their personal data. Organizations must also implement appropriate technical and organizational measures to protect personal data against unauthorized access, alteration, or destruction.

Thus, the objective of the right to data protection is to protect personal data and ensure that it is collected, used, and stored in a way that respects individuals' privacy rights, giving individuals control over their personal data, including the right to access, correct, delete, and object to the use of their personal data for certain purposes, and also imposing obligations on organizations that collect and process personal data, such as obtaining explicit consent, informing individuals about data usage, giving them control over their personal data, and implementing appropriate measures to protect personal data against unauthorized access, alteration, or destruction.

Therefore, the principle of purpose, the principle of adequacy, the principle of necessity, the principle of free access, the principle of data quality, the principle of transparency, the principle of security, the principle of prevention, the principle of non-discrimination, and the principle of accountability and accountability are thus constitutive elements of the right to personal data protection, and not additional conditions. Still, regarding the content, it is noteworthy that it is identical to that of informational self-determination, which is a decision right, whose object would be the care of data and information related to a particular person.

Finally, it is worth mentioning that according to the legislation, there is no differentiation between the terms "information" and "data", but rather, if there is the identification of a natural person. Nevertheless, it is always worth remembering that academia has already clarified the exactness of each of these terms.

Thus, it is concluded that the right to personal data protection should be understood as a new right to personality, since these same data influence the individual's projection and their relational sphere with the world.

The Right to Personal Data Protection is a new right, which mainly arises from the incessant search for personal data by States and Private Companies in the need to monetize, turning them into highly profitable raw material and product. As Shoshana taught us, surveillance capitalism is primarily based on the expropriation of the most basic human rights, such as autonomy and freedom, through the extraction, prediction, and sale of people's data.

In this scenario, the elevation of the Right to Personal Data Protection to a fundamental right serves as a systemic defense of checks and balances that are embodied to express society's stance in

the face of personal data processing. Thus, the recognition of a subjective right of constitutional scope.

By this corollary, the Right to Personal Data Protection can be defined as an instrumental/ procedural and substantive right. Data protection is primarily a transparency tool, but sometimes its substantive provisions restrict the possibility of processing personal data or establish limits on the types of processing that can be done on personal data. Personal data protection is intended to enable a wide range of rights and freedoms, such as privacy. Being a right that aims to provide proactive and structural protection of the rights and freedoms that may be affected by the processing of personal data.

Repeat. The principle of purpose, necessity, free access, data quality, transparency, security, prevention, non-discrimination, accountability, and accountability are constitutive elements of the right to personal data protection. Nevertheless, it is worth emphasizing that these elements are not unique to constitute the right. The right is dynamic and constitutes a synthetic representation of the social stance that has developed over the years, in response to the diffusion and importance that the processing of personal data has acquired since the turn of the century.

Data protection can be considered both a substantive and procedural right. Substantive data protection refers to the protection of an individual's personal information, including rights of access, rectification, or erasure of personal data and the right to object to the processing of their personal data. It also includes the right to privacy, which is the right to control who has access to personal information and for what purpose it is used.

Procedural data protection refers to the processes and procedures that organizations and governments must follow to ensure that personal data is collected, stored, and used in compliance with data protection laws and regulations. This includes requiring organizations to have clear and transparent privacy policies, obtain informed consent before collecting personal data, and notify individuals and authorities in case of data breaches.

Thus, it refers to a combination of substantive and procedural rights. Substantive rights ensure that individuals have control over their personal information and procedural rights ensure that organizations and the government follow specific procedures to protect personal data.

Therefore, to understand the essence and logic of a right, one can also start from its violation: a violation of purpose specification or rights of access and rectification, or the control of the independent authority, does not necessarily equate to a violation of the essence of the right to

personal data protection itself. It is explained that personal data protection is intended to enable information sharing: there would be no need for this if there were a general prohibition on disclosing personal data, and the law rarely prohibits the processing of personal data, but obliges processors and operators to meet requirements, to do so legally. This permissive conception of the right to personal data protection as a transparency tool is consistent with its procedural nature.

In this sense, it is recalled that in many circumstances of modern life, an individual may wish to waive part of that control or make their personal data available to the public and/or private organization that offers a desirable service/product to them. In this vein, the sharing of personal data for a benefit is not inherently unfair, as long as both parties have clarity and transparency about the terms of this exchange and comply with the law. As elaborated in this thesis, the implications of the right to personal data protection in today's world have ramifications in virtually all other existing rights. The right to personal data protection can identify and be applied to transatlantic sharing of personal data, mass surveillance, mass collection and/or retention of data, by the State or private companies, as well as in cases of monitoring and filtering electronic communications to prevent copyright infringements, to the transmission of personal data on a website accessible to anyone on the internet. In contrast, copyright protection primarily concerns the safeguarding of intellectual property rights, particularly in creative works and expressions. Acts such as copying, distributing, or reproducing copyrighted material without authorization constitute copyright infringement. While the right to personal data protection focuses on safeguarding individuals' privacy and controlling the use of their personal data, copyright protection pertains to the protection of creators' rights over their intellectual creations. The two legal concepts operate in distinct domains, with personal data protection primarily concerned with privacy rights and data control, while copyright protection revolves around intellectual property rights and the prevention of unauthorized use or reproduction of creative works.

Individual control over personal data is desirable from a conceptual perspective. It is fundamental for individual self-development and can help minimize power and information asymmetries. Individual control should not, therefore, be absolute. Instead, it is suggested that individual control over personal data should function as a starting point for the analysis of personal data processing: individuals should have control over their personal data unless there is a legally accepted third-party interest in processing. Thus, personal data processing must ensure compliance with principles and safeguards for respecting individuals' rights. Implicit in this framework is,

therefore, a reconciliation of the rights of data subjects with the interests of those processing personal data and of society, more generally.

However, the burden of proof falls on the data controller responsible for demonstrating the limitations on the data subject's right. This is justified based on the subjective dimension, which seeks precedence over the interests of personal data controllers. The starting point in the application should be individual control over personal data, as it does not require the data subject to demonstrate a legitimate reason to object and instead requires the controller to justify the need/purpose of processing, especially when dealing with sensitive personal data.

Thus, it can be affirmed that the right to personal data protection has acquired the attribute of a fundamental right and is fully applied to the constitutional-legal regime, in both material and formal senses: 1) it has become an integral part of formal constitutionality, with normative status superior to supranational legal order; and, finally, and most importantly, 2) its essence is endowed with immediate applicability (direct) and directly binds the actors.

It is concluded, therefore, that the Right to Personal Data Protection is a fundamental right, with the characteristic of an instrumental/procedural right, which serves as a transparency tool, designed to provide safeguards to the individual whenever their personal data is processed. Personal data protection is also a procedural/instrumental right, insofar as it hardly protects a specific interest, but serves the objectives pursued by other substantive fundamental rights, such as human dignity and/or privacy. Time and reflection will serve as a process of adjusting the law in 21st-century society. It is certain, therefore, that national legislation and the Supreme Court hold defined rules and norms that allow protecting the individual citizen and society, with authorities, society, and the judiciary dealing with arbitrary or abusive practices in the coming decades, which we may observe in future academic work that allows for a comprehensive overview of the subject in daily practice.

The right to personal data protection, therefore, is a fundamental right to the protection of the human person and their dignity with the foundations of the legal and normative bases of the due informational process in the face of existing conflicts in the information society and the era of surveillance capitalism.

The tectonic movement of creation, modification, and assimilation of personal data protection has deeply impacted the legal landscape, triggering a frenzy among scholars, authorities, and the curious. Suddenly, capitalism has transformed into surveillance capitalism, and pandemic-fighting mechanisms have become instruments of privacy invasion. Artificial intelligence emerges as the last

frontier of a wave of new opinions, all based on cyber-legal concepts, turning data protection into a battleground where there is no middle ground: either one accepts the collection and secondary sharing of personal data, even without the consent of the data subject, or activities come to a standstill. In this context, data protection, its logic, and discourse have presented discouraging results.

Similar problems arise regarding fundamental concepts of the data protection system. The law should require a purpose in the collection, but reality responds with the increasing combination of databases, often in an automated way, making this legal requirement illusory. The law should determine that processing should use the minimum necessary data, while reality contradicts, with the global volume of processed data increasing exponentially every year. The most concerning result is that the data protection system does not work in practice, generating bureaucratic problems and legal conflicts on a global scale.

Mutual Legal Assistance, a mechanism enabling the prosecution of Transnational Organised Crime: barriers and solutions

Thomas Delorme

SORBONNE DOCTORAL LAW REVIEW
REVUE DOCTORALE DE DROIT DE LA SORBONNE
Vol. 7 n°1

TABLE DES MATIERES

Résumé

L'essor du crime organisé transnational constitue une menace internationale fondamentale et nécessite des mécanismes efficaces de poursuite, sans lesquels ces entités illégales éroderont les capacités de l'État. Cet article explore l'idée que la coopération entre les États est la seule façon de prévenir l'émergence de refuges sûrs pour les criminels. En retraçant l'évolution des Traités d'Assistance Juridique Mutuelle qui codifient les conditions dans lesquelles les forces de police échangent des renseignements et des preuves, cet essai met en lumière à la fois leur importance cruciale et leur application décevante. Les obstacles persistants à cette approche multilatérale ont poussé les nations à forger des traités bilatéraux d'assistance juridique mutuelle et à explorer des canaux alternatifs d'échange d'informations, y compris des mécanismes extraterritoriaux et parfois illégaux, au détriment de la souveraineté et de la confiance mutuelle.

Malgré des progrès normatifs alimentés par une approche dirigée par Washington, les refus discrétionnaires soulignent la nécessité de réduire davantage les possibilités de rejet. Alors que l'absence de politiques de renforcement des capacités stables et soutenues sur une base bilatérale a été partiellement compensée par l'influence croissante de l'Office des Nations Unies contre la Drogue et le Crime (ONUDC), un problème plus profond persiste : la méfiance entre les nations. L'examen de régions telles que l'Amérique latine et l'Union européenne révèle des développements prometteurs sous la forme d'institutions plus intégrées, offrant une clé potentielle pour réduire l'influence omniprésente de la méfiance dans les procédures transnationales. En pratique, cependant, les approches unilatérales et extraterritoriales sont devenues prédominantes, éloignant encore davantage la perspective de développer une confiance mutuelle entre les États. Cet article identifie non seulement les défis existants dans le domaine de l'assistance juridique mutuelle, mais plaide également pour des efforts continus visant à renforcer la coopération internationale face à la menace redoutable posée par le crime organisé, en identifiant et en évaluant des solutions potentielles.

Abstract

The rise of transnational organised crime poses a fundamental international threat and necessitates effective mechanisms for prosecution, without which these illegal entities will erode the capacities of the State. This paper explores the view that cooperation between States is the only way to prevent the emergence of safe havens for criminals. Tracing the evolution of Mutual Legal Assistance Treaties (MLATs) which codify the conditions in which police forces exchange intelligence and evidence, this essay both highlights their crucial importance and their disappointing application. Persistent barriers to this multilateral approach have led nations to forge bilateral MLA treaties and explore alternative channels for information exchange, including extraterritorial and sometimes illegal mechanisms, at the expense of sovereignty and mutual trust.

Despite normative progress fuelled by a Washington driven approach to the issue, discretionary refusals underscore the need to further diminish the scope for rejection. While the absence of stable and sustained capacity-building policies on a bilateral basis has been partially compensated by the growing influence of the United Nations Office on Drugs and Crime (UNODC), a deeper issue persists—distrust among nations. Examining regions such as Latin America and the European Union reveals promising developments in the form of more integrated institutions, offering a potential key to reducing the pervasive influence of distrust on transnational proceedings. In practice, however, unilateral and extraterritorial approaches have come to the forefront, further driving away the prospect of developing mutual trust between States. This paper not only identifies existing challenges in the realm of Mutual Legal Assistance but also advocates for continued efforts to fortify international cooperation in the face of the formidable threat posed by organised crime, identifying and evaluating potential solutions.

Introduction

'The threat to our security is not in an enemy silo, but in the briefcase or the car bomb of a terrorist. Our enemies are also international criminals and drug traffickers who threaten the stability of new democracies and the future of our children.'

Bill Clinton's 1995 address at the United Nations (UN) Fiftieth Anniversary Charter Ceremony highlights his era's growing concern for a previously neglected issue. It came at a time when organised crime was gradually becoming an international priority, and represents growing awareness that in a globalised world, criminals had become a common enemy (Annan, 2003). The UN Office on Drugs and Crime (UNODC) has estimated the revenue generated by organised crime to represent 2 to 5% of world GDP (Cryer, 2010). Interpersonal, gang and organised crime-related violence kills more people than political violence globally (Albanese, 2018). States have collectively identified the issue and have since attempted to develop legal formulas to remedy the situation.

André Bossard, former Interpol director, defines transnational crime as acts 'necessitating the cooperation of two or more countries to solve, either because the crime itself is transnational insofar as it implies crossing at least one border before during, or after the fact, or by the consequences or the transnational character of the crime' (Madsen, 2016, p.1) International cooperation is rendered crucial by the inherently cross border nature of transnational organised crime (TOC), and the failure of authorities to work hand-in-hand invariably leads to the establishment of safe havens, as criminals profit from enhanced mobility of a globalised world to escape prosecution (Harfield, 2003). To remedy the situation, States can call on their partners to share information with them and execute part of an investigative procedure. These acts of cooperation are known as mutual legal assistance (MLA), defined in the UN Convention Against TOC (UNTOC) as "widest measure" of cooperation "in investigations, prosecutions, and judicial proceedings' (art. 18). Significant barriers impede the effective application of MLA. Analysed in Section 1, they are multifaceted and cover several legal obstacles. The international community has attempted to overcome such limitations, and these attempts will be the focus of Section 2. Issues of legislation have been overcome through criminalisation, yet extra-legal barriers are far harder to tackle, as some States lack the capacity to implement the ambitious provisions of UNTOC and other treaties, whilst garnering trust between nations has proven to be an almost insurmountable challenge. International cooperation in criminal matters is fundamentally heterogeneous. Its application therefore cannot be grasped simply through the analysis of treaties but calls for a study of how it has been implemented. Section 3 will therefore discuss effective application of MLA in practice, demonstrating that lasting barriers lead countries to develop bilateral MLA treaties (MLAT) and when possible, obtain information through alternative channels. The United States' and China's approach to gathering evidence highlight the gaps of MLATs, as they make use of its extraterritorial reach and dominance in strategic sectors to obtain information for prosecution, acts which undermine sovereignty. Nonetheless, further integrated models of MLA have developed, providing evidence that seemingly insurmountable obstacles can in fact be overcome. If the European Union, through its high-level of homogenisation is a fertile ground

for such cooperation, the Latin American region, due to its high exposure to TOC and its consequences, has conceived innovative responses which could serve as inspiration to overcome barriers on a global scale.

The essay picks up on, an albeit limited, literature evoking solutions to strengthen the existing MLA system or seek alternative ways to reach its objectives. Ranging from suggestions to create a supranational arbitration system to deal with MLA request denials to the development and generalisation of crime-based sanctions as a way of denying safe havens, these potential innovations all have their strengths and drawbacks. When they are ambitious, they will most likely never garner international support, and when they are feasible, they may risk infringing upon individual rights. When dealing with MLA, it is worth remembering that when discussing a potential change in the system: "if it is good, it will not be signed by all relevant parties, and if it is signed by all relevant parties, it will not be good" (Woods, 2017, p.670).

Section 1: Analysing conceptual barriers to Mutual Legal Assistance

1.1 The persistence of discretionary refusals and their embeddedness within the international system

International transfers and collection of evidence as a way of guaranteeing prosecution despite the presence of a foreign element in the procedure pose a considerable set of challenges to overcome. Denying safe havens relies on reducing the efficacy of fleeing the jurisdiction in which a crime was committed as a strategy to escape prosecution. This requires authorities to be able to cooperate on primary and secondary forms of MLA (Vries, Anderson, 2022); the former refers to proactive operations which include a transfer of procedural responsibility such as seizing assets or collecting evidence on behalf of the requestee, whilst the latter simply involves sharing existing evidence or intelligence. Although in principle all States share organised criminals as common antagonists, they also share the desire to maintain control over sensitive information and sovereignty over their jurisdictions. This tension between cooperation and sovereignty has allowed for contradictory tendencies associated with the development of MLA frameworks to overlap and prosper.

If transnational organised crime became an international priority during the 1990s (Fijaut, Paoli, 2008), difficulties persist to this day in creating a harmonised system for States to request both primary and secondary forms of MLA. If political and mutual trust between States remains the central barrier (Section 2.2), legal motives for refusing cooperation are embedded in the treaties themselves, whether they be multilateral, i.e. UNTOC, or bilateral MLATs. These motives appear as safeguards, all crucial, yet some are instrumentalised to enable discretionary rejections of cooperation. Those that protect individual human rights are particularly important to uphold without exception. For instance, in *R (El Gizouli) v Secretary of State for the Home Department [2020] UKSC 10*, the prosecution of Maha El Gizouli for terrorism after his arrest in Syria in 2018 by the United States depended "critically" on evidence collected by UK law enforcement. The UK Supreme Court found that "it is unlawful at common law for the state to facilitate the execution of the death penalty against its citizens or others within its jurisdiction anywhere in the world" ([143]), asserting

sovereignty over the collected evidence and promoting its human rights regime. Political exceptions to MLA requests must also be continuously upheld to prevent attempts to instrumentalise the system to repress political opponents and dissidents, as is the case with regard to FATF standards or Interpol Red Notices (Reimer, 2024).

If human rights rejections are necessary to avoid weaponizing the international system, certain exceptions can be instrumentalised for the opposite purpose: refusing to share requested information, to execute an investigative procedure or to freeze assets without having to explain the decision. The Djibouti v France ICJ decision demonstrates such arbitrary tendencies, a case in which France refused to comply with a request made based on a provision included in a bilateral treaty by citing its national security interests and the ICJ ruled that Djibouti could not contest the unilateral decision [135]. The ruling contends that that the "requested State enjoys wide discretion in deciding to refuse mutual assistance" if it "considers that execution of the request is likely to prejudice its sovereignty, its security, its *ordre public* or other of its essential interests". The ruling considers this to be "self-judging clause", as long as the requested State acts in good faith. Yvon Dandurand and Jessica Jahn highlight the issues behind the "self-judging clause": States can refuse or ignore cooperation requests without there ever being any kind of recourse made to them. They contend that only "radical" reforms, such as the establishment of a "binding arbitration mechanism to resolve bilateral disputes" could help save a failing system (Dandurand & Jahn, 2021, p.14). Such a mechanism could involve a possibility to appeal to a supranational authority to appeal to when a request for MLA is denied or simply ignored. Inspiration could be taken from international investment law, more specifically clauses included in bilateral investment treaties that provide arbitration conditions upon signature.

1.2 Coexistence of opposed legal philosophies: Mutual Legal Assistance between Common and Civil Law jurisdictions

Barriers to MLA can arise when discrepancies in legal systems and philosophies complicate the exchange of information process to such a point that assistance requests are delayed, denied, or lead to evidence being declared inadmissible in court when the *modus operandi* fails to conform to domestic legislation. The interaction between Common and Civil law jurisdictions illustrates this conflict of systems. Historically, given the geographic specificities of Common law jurisdictions, their utilisers were slow to build MLA relationships, both because it appeared pragmatic to them that the State in which prosecution took place would be best suited to gather evidence, and due to a general reticence to enforce another State's norms, thus viewing assistance through a sovereignty lens (Boister, 2018). Civil law systems in continental Europe, on the other hand, found MLA to be of use given population mobility. The differences in legal cultures, widely present in most areas of law, extend to MLA (Boister, 2018).

One prominent aspect of the Common and Civil law divide concerns the way in which evidence is gathered, and although the US has developed a doctrine of "double illegality" (see Section 3.1), issues of admissibility of evidence can arise due to different processes of evidence

collection. An illustration of this and how it affects prosecution of TOCs can be found in the prosecutions resulting from *Operation Venetic,* where the UK was given access by a French and Dutch Joint Investigation Team to millions of compromising messages exchanged between criminals on encrypted phones (Europol, 2020). Across Europe, questions were raised over rights of the defence, as the methodology used by French authorities was kept secret due to national security concerns, thus limiting the possibility for defendants to question its legality. In France, the Constitutional Court was called to statute on the question of which balance to strike between the principle of equality of arms between defence and prosecution and the necessity to protect national secrets (Ascione Le Dréau, 2022). In the UK, litigation mostly concerned the nature of the evidence, and more specifically whether the communications were intercepted whilst being stored or being transmitted (Griffiths, Jackson, 2022). Contrary to continental Civil Law jurisdictions, intercept material in the UK was historically used for intelligence purposes but would not be admissible in court. The 2016 Investigatory Powers Act alleviated this restriction, enabling prosecution to use intercept material when it is "stored in or by a telecommunication system" (Section 6(1)(c)(i)). In the case of *Operation Venetic,* courts held that the information was obtained whilst "being stored", rather than "being transmitted", and such a ruling could pave the way for further use of such material in cases concerning TOC (Section 6(1)(c)(i)). These legal developments suggest that the gap is being bridged and inconsistencies are thinning, allowing for MLA to transcend systemic discrepancies. Nonetheless, procedural differences remain. The "golden evidence rule" is an example of this, as Common law jurisdictions require authorities to be able to justify that the evidence has been sealed and protected from the moment of collection until trial. This can lead to it being declared inadmissible in courts, as foreign officers lack the training or the knowledge to fulfil the requirements (Madsen, 2016).

The relationship is not however systematically one of opposition, as jurisdictions can also take inspiration from one another as they develop their response to TOC (Balsamo, 2016). For instance, European scholars have called for their jurisdictions to integrate non-conviction-based confiscations, present in Common law jurisdictions in the form of civil forfeiture, which allows governments to seize any property allegedly involved in a crime or illegal activity. As such, non-conviction-based confiscations could be part of a strategy to make the law more flexible.

1.3 Regulating TOC within the confines of the rule of law

An effective rationale to justify an obligation to provide MLA can be derived from an International Human Rights Law requirement to investigate, prosecute, and adjudicate conduct harming citizens (Vervaele, 2014), thus constituting a responsibility to protect citizens from transnational criminals. However, such an argument necessarily raises the issue of conflicting rights, as a balance must be struck between protecting citizens and guaranteeing a fair trial to the defendant (Brems, 2014). States have found it difficult to strike such a balance, as MLA tends to predominantly favour the interests of

the State, this is the case in jurisdictions that actively promote rights of defendants, and even more so in jurisdictions that do not possess such safeguards.

In the context of transnational proceedings, the equality of arms principle, which requires each party to be given a reasonable opportunity to present their case under conditions that do not place them at a substantial disadvantage (Gless, Vervale, 2013), is often disregarded, as the possibilities offered by MLATs are only available to States. Scholars highlight the fact that defendants in transnational proceedings operate within a judicial "black hole" (Gless, Vervale, 2013, p.6), as the rules of the game, particularly concerning admissibility of evidence are often modified. Such modifications are particularly prominent in US and EU jurisdictions. In the US, *The Ver*dugo case created a "double illegality" requirement (Bentley, 1994) in which Fourth Amendment rights could be bypassed by obtaining evidence abroad (see Section 3.1). In the EU, German, French and crucially, European courts have opened the door to similar admissibility criteria. For instance, the *Bundesgerichtshof* accepted the use of a witness statement obtained in Turkey without the presence of a lawyer for the defence, even though such evidence would be excluded had the interview taken place in Germany [4 StR 126/92]. In *Stojkovic v France and Beligum,* French authorities had made an MLA request for an interrogation concerning a detainee in Belgium who was subsequently questioned without the presence of a lawyer, which, according to his status as a *témoin assisté* (intermediate status between a witness and a defendant under French criminal law) which would have given him the right to such assistance in France. The breach was crucial to the outcome of the case as the defendant gave incriminating evidence in that specific interrogation. Despite ruling that French and Belgian authorities had breached article 6 of the European Convention on Human Rights (ECHR) pertaining to the right to a fair trial, France was only ordered to pay non-pecuniary damages to the applicant, and the EctHR (European Court of Human Rights) failed to weigh in on whether such evidence was admissible. These cases highlight an uneasy coexistence of guarantees available to defendants and transnational proceedings in which rules are modified in the interest of pragmatism. This is particularly relevant in the EU, where mutual recognition of evidence is stipulated in Article 82 of the Treaty on the Functioning of the EU (TFEU). Combined with the existence of policing and judicial networks such as Europol and Eurojust, the integration model allows for forum shopping (Gless, 2013), a practice in which States prosecute in the jurisdiction most likely to award them a favourable outcome. In the US, these inherently unfair consequences are embedded in MLATs themselves, as they were designed for law enforcement. An intention to extend their access to defence lawyers never materialised. In this regard, disallowing an accused person to search for exculpatory evidence abroad was part of a "tough on crime" stance (Richardson, 2008), in which the balance struck concerning conflicting human rights heavily swayed towards potential victims. According to Richardson, the imbalance is the product of majoritarian bias, in which the majority protects its interest by applying a policy that "harms the minority group far more than any corresponding benefit to the majority" (Richardson, p.93).

The design of MLATs sways heavily in favour of States on the global stage and even more so in jurisdictions with less concern for individual human rights. This stems from the fact that UNTOC's

article 18, the "mini treaty" on MLA", does not create specific due process or fair trial rights; instrad, it includes a passing reference to "due regards to the rights of the defence", rather such rights will vary depending on the adherence or lack of to specific international agreements. China has for instance signed an MLAT and a "Boundary Management System" with Nepal, designed to "expedite" both extraditions and increase surveillance of Tibetan refugees (Freedom House). The agreement contributes to the denial of jurisdictional safe havens, with political and individual rights bearing the brunt.

Section 2: Evaluating attempts at creating a harmonised international framework for Mutual Legal Assistance

2.1 Promoting convergence of domestic legislation through criminalisation

Despite the absence of a strict dual criminality requirement in most bilateral and multilateral treaties, discretionary refusals and exceptions to the rule highlight the need to harmonise domestic regulations to reduce the scope of such occurrences to promote cooperation. The process of criminalisation responds to a two-fold requirement to incorporate the transnational nature of organised crime and to monitor the evolution of compliance. The 1990s was a decisive decade in this regard, as previously disregarded acts such as money-laundering and bribery of foreign officials were recognised as key enablers of TOC and became international priorities. The 1988 Vienna Drug Prohibition Convention signalled a turning point as it integrated the proceeds of crime into international policy (Nadelman, Andreas, 2008), seeking to "establish as criminal offences under its domestic law, when committed intentionally" (art.3). The voluntarist nature of International Law and the overwhelming adhesion to codifying treaties, of which UNTOC and UNCAC are prime examples (signed by 191 and 189 parties respectively), obscures the reality that criminalisation emerged not as a natural worldwide response to the issue of TOC, rather a result of the actions of "transnational moral entrepreneurs" (Nadelman, Andreas, 2008) which decisively shaped the process as they imposed a specific body of norms internationally. These treaties were heavily influenced by norms already present within certain legal systems. Samuel Witten, legal advisor to the State department, argued for US ratification of UNTOC by positing that "the value of these Convention provisions to the United States is that they oblige other countries that have been slower to adapt to the threat of transnational organised crime to adopt new laws in harmony with ours" (Boister, 2018). Criminalisation thus provides the benefit of constraining parties to legislate in a way that is consistent with US norms. However, these treaties left transposition to the goodwill of domestic authorities, and a review mechanism to survey its implementation was only launched in October 2020. Concerning UNCAC, a group including Russia, China, Iran, Pakistan, Venezuela, and Ecuador argued in favour of national discretion for implementation and the refusal of a review mechanism (Heimann, 2018). Faced with this resistance, non-State "transnational moral entrepreneurs" (Nadelman, Andreas, 2008) affiliated to a Western conception of TOC paved the way for the "Washington consensus" (Krastev, 2000). The World Bank and the International Monetary Fund led similar policies, as they began to include anti-money laundering evaluations in country evaluations, as well as including bribery and corruption as

part of their selection mechanism for loans and contracts. These highly effective harmonisation mechanisms led to the criminalisation of drug trafficking facilitation practices such as bank secrecy, formerly considered to be an acceptable practice of customer confidentiality (Levi, 2002). Harmonisation through criminalisation has been the main success of the 1990s and the 2000s, creating the conditions for evidence to be shared without the obstacle of the dual criminality requirement. Legal uniformity in fact contributed to the requirement being dropped in many MLATs. The process was heavily influenced by US policy, and not only explains the content of the treaties, but also helps fathom its subsequent application. Harmonised definitions facilitated requesting MLA yet failed to address issues of capacity (Section 2.3), creating a discrepancy between the ambition of the treaty and its effective application. Ironically, the US, which was the main advocate for criminalisation, has itself been a victim of such an uneven process, overwhelming signatories of MLATs with demands and having to employ extraterritorial methods to obtain them (Section 3.1).

The Financial Action Task Force (FATF) has since emerged as the key regulator in the realm of finance and security. Created in 1989, it published 40 recommendations to combat money laundering and corruption. Despite the FATF comprising of only 39 member-states, it developed a "naming and shaming" policy to expose those who failed to comply with the recommendations, to such a point that countries would do anything to make sure we are not on that list, fearing economic consequences. If the FATF has emerged as a strong normative actor with regards to, for instance, implementing norms in relation to banking intelligence, it has not yet adopted a proactive role in enforcing MLA. Although lacking standards in terms of MLA are part of the mutual evaluation process, by which countries can be listed as jurisdictions under increased monitoring. South Africa was placed on the list in the latest update provided by the Paris based institutions in June 2024, with a mention made of its deficiency regarding "outbound mutual legal assistance" (FATF, 2024). Other countries have had similar remarks made to them, including the United Arab Emirates (UAE), notoriously a haven for transnational criminals, as recently demonstrated by the Dubai Unlocked journalistic investigation. To obtain its removal from the so-called "grey list", amongst other measures, the UAE signed 44 bilateral MLATs and sent out 327 requests for information, achieving its objective in February 2024 (Francis & Odeyaji, 2023). The UAE example demonstrates that the FATF functions as a simple compliance mechanism, ticking numerical boxes rather than assessing MLA standards qualitatively. Indeed, as extradition requests for criminals arrested in Dubai have been ignored (Ljubas, 2024), it is difficult to imagine Dubai suddenly becoming a reliable partner for MLA. Yet, the UAE's major efforts to free itself from the FATF's high scrutiny jurisdictions signals the institutions high normative and de facto enforcement capabilities. If it were to heighten its qualitative standards with regard to MLA, it could spearhead meaningful change.

2.2 The impossible task of nurturing mutual trust

Information exchanged via MLA is inherently sensitive, as it contains intimate data concerning individuals and ongoing investigations. States executing requests are therefore trusting their

counterpart to maintain the confidentiality of such information and that it be used appropriately, thus respecting the principle of speciality that dictates that evidence received must be used exclusively within the boundaries of the reasons for which it was requested. Two forms of trust therefore emerge, the first regards the capacity of States to maintain confidentiality, the second relates to the diplomatic relations entertained with the requestee and the belief that it will respect the principle of speciality. A Senior Official in the UK's Serious Organised Crime Agency illustrates this fact by admitting that "the sad truth is I am not going to share my best, most delicate information with the Russian or Mexican police departments" (Naim, 2012, p109). Russia launching a full-scale invasion of Ukraine has completely undermined any prospect of international cooperation and illustrates a trend of wavering multilateralism in the context heightened geopolitical tensions, compromising international cooperation. This provides an explanation to difficult China-US cooperation in the context of the fentanyl crisis, as a US congressional report points to "Many outstanding requests by both the United States and China remain unfulfilled" (Greenwood & Fashola, 2021, p. 8). Mass corruption in Mexico's government, illustrated by the recent conviction of García Luna, formerly responsible for Mexico's response to cartels, highlights the fear of confidentiality concerning "sensitive operational information" (*Travaux Préparatoires,* UNODC, p.269). The nexus between capacity and trust explains why cooperation is mainly reserved to "prosperous and peace-loving nations that have an effective public administration" (Fijnaut, 2000, p.125). As the *Djibouti v. France* caselaw suggests, even the existence of treaty obligations cannot compensate for trust when dealing with sensitive information. Proactive forms of MLA implicate delegation of a procedural responsibility, meaning that the requesting State must be confident in the executing State's capacity to seek out evidence whilst respecting a process that may differ from their own jurisdiction.

The consequence of international distrust is not only that MLA is often an exclusive and bilateral club, but also that it mainly operates thanks to informal connections between law enforcement officials (Boister, 2003). Due to the difficulty, if not the impossibility, of obtaining evidence through MLA requests, such information is often obtained outside the framework of MLATs, and an official request will only be made when evidence is needed for trial (Perras, 2017). Under this model, liaison officers are vital, fulfilling the role of information gathering diplomats. Informal connections create a relationship of dependence between the human qualities of the liaison officer and information gathering. As such, a need to resort to affinities between individuals testifies to the weakness of current MLATs and information sharing mechanisms. Only in the EU are such relationships automatised, through the development of "detailed cooperation frameworks" (Hufnagel, 2017, p.32) such as the Schengen Information System which operates as a collaborative database, as a threshold of trust has been established (Section 3.3).

2.3 Enabling the transition from theory to practice through capacity building

To enable effective cooperation legally possible thanks to the convergence of domestic legislation, treaties established that signatories would "designate a central authority that shall have the

responsibility and power to receive requests for MLA and either to execute them or to transmit them to the competent authority" (art 18(13)). It was agreed that countries were unequal in their ability to comply to such measures, given that some nations possessed pre-existing infrastructure or had more means to build them. Therefore, capacity-building clauses were integrated into suppression treaties as part of the negotiations, as a condition imposed by nations of the Global South to change their practices and laws. The UNTOC therefore provided "to enhance financial and material assistance to support the efforts of developing countries", which was to be done to the best "extent possible" (Article 30(2)(b)). The process of capacity building is fundamental to developing MLA, not only because scarcely resourced systems and poorly trained personnel are unable to deal with the flow of requests, but also due to the sensitivity of such information, as States feared that the confidentiality of such information would be compromised. This exact concern was formulated during the *travaux préparatoires,* as the issue of sensitive operational information was raised, particularly concerning ongoing investigations, illustrating the link between capacity and trust. Capacity-building initiatives seemed mutually beneficial, allowing for countries lacking centralised headquarters to develop the necessary infrastructure, and for countries desiring to make use of the newly established framework to share and request information without fearing for its confidentiality. Nonetheless, efforts for development have failed to materialise, as the African group at the 2015 UN Commission on Crime Prevention and Criminal Justice called for more technical assistance, and in the same year, at the Conference of State Parties to the UNCAC, 59 of such Parties identified over 2,200 technical assistance needs. Such limitations highlight a huge gap between the ambitions of the suppression treaties and their effective implementation (Fijnaut, 2000). Section 2.1 identified that faced with the issue of criminalisation, transnational moral entrepreneurs led by the US adopted an aggressive strategy, which is only partially possible in relation to capacity building. In this instance, States with greater resources are tasked with a development responsibility yet cannot be constrained into acting as the UNTOC only provides for best efforts obligations. Thus, efforts were mainly bilateral and purely self-interested, as part of a "first-line of defence" strategy. For instance, a US initiative assisted Haiti in re-creating its civilian police force, yet new stations were primarily located on the West Coast due to it being an area used by Columbian cartels for trafficking (Boister, 2018). As funding capacity-building is voluntary, countries operate under the threat of resources being stripped and distributed elsewhere. In part because of the highly targeted nature of bilateral assistance, the UNODC has attempted to fill the void by providing a multilateral conduit focused on developing competencies and training, by familiarising relevant personnel with the legislation and framework (Boister, 2018). The UNODC's contribution was recognised by the General Assembly (Resolution 73/186), identifying the progress made in the delivery of advisory services and technical assistance. A crucial factor towards enabling cooperation, capacity-building is limited by the discrepancy between the ambition of treaties and the funding effectively attributed to their implementation.

Section 3: The regional and heterogenous reality of Mutual Legal Assistance: from bilateralism to integration

3.1 The temptation of circumventing MLA through extraterritorial collection of evidence

The US's approach to MLA showcases limitations within the multilateral system as it makes use of its extraterritorial reach to circumvent procedural barriers and even breach its obligations under international law. In spite of international suppression treaties and a multitude of bilateral agreements, the US faces difficulties obtaining all the evidence it needs to pursue prosecutions of a transnational dimension. Its MLATs with Central and Southern American countries, which have overloaded domestic courts with requests, demonstrate the discrepancy between the US's ambitions and the limited capacities of some of its partners (Harfield, 2003). This serves as a justification for US authorities to conduct its own evidence gathering operations abroad, rather than remaining within the boundaries of MLATs which provide for a transfer of procedural responsibility, as a corollary condition to State sovereignty. The leading case discussing the rationale behind the method can be found in *United States v Verdugo Urdiquez* [494 U.S. 259 (1990)]. It purports to a joint operation led by the DEA and Mexican Officials in which premises belonging to the Mexican defendant were searched without a warrant and the evidence was subsequently used for a conviction in the US. The Supreme Court found that rights awarded by the Fourth Amendment of the US constitution regulating unreasonable searches and seizures did not apply to "a non-resident alien located in a foreign country" [23], and that applying such a right would disable "political branches to respond to situations involving our national interest."[22] "National security" refers to a vague and permissive standard and the Court's jurisprudence *de facto* liberalised the use of such evidence. The Court's decision creates a "double illegality" requirement, requiring that the procedure violate the search standards of both the US and the concerned country (Bentley, 1994). The pragmatic rationale of such a decision is to restrict situations in which evidence could be disregarded by courts on the basis of a procedural discrepancy. An adverse corollary effect of such a doctrine is that it encourages an extraterritorial approach, precisely in order to escape constitutional obligations. The *Verdugo* case further demonstrates an extraterritorial tendency as the search violated Article (1)2 of the drafted US-Mexico MLAT which expressly forbade the exercise of sovereign powers within the other party's territory, although the treaty was in fact only signed and ratified after the dispute arose. Nonetheless, the US acted incompatibly with treaty obligations, further highlighting the irreplaceable role that trust in the corresponding administration plays when choosing a *modus operandi.*

Undoubtedly, the US is able to act in such a manner due to its status and hegemony in so many domains, a key one being digital platforms. Due to most major social media platforms being based in the US, it is likely that user information is stored on its territory, including incriminating data necessary for prosecution. US municipal law prohibits firms from disclosing most customer content except in response to a warrant issued by a domestic judge (Nojeim, 2015). As an exception to these blocking statutes, US law allows for firms to hand over metadata, yet the standard practice has been for these corporations to reject such demands, hiding behind aforementioned blocking statutes and customer privacy. The consequence of this dominance is that foreign jurisdictions are dependent on

the US's goodwill to share information exchanged between their own nationals, and also that US authorities have direct access to foreign conversations without even having to submit an MLA request. The line between extraterritorial reach and the benefit of possessing a dominant position seems an unclear one, yet both point towards the US's ability to obtain evidence through multiple channels, thus bypassing requirements stated in MLATs.

In terms of long-arm and extraterritorial reach, the People's Republic of China (China) has taken matters even further by setting up covert police stations abroad that fully encroach upon sovereignty, the most publicised example being in Manhattan (US Department of Justice, 2023). These covert facilities and agents have been utilised to coerce into forced returns and intimidate dissidents, but also to with build cases on corrupt officials and petty criminals, fully embedding the practice within a strategy of circumventing traditional MLA.

These examples suggest an inexorably worsening landscape, yet this is not the only way forward. In R (KBR, Inc) v Director of the Serious Fraud Office, the UK Supreme Court found that law enforcement acted wrongfully by using channels outside of the MLA framework (Cochrane, 2022, p. 528). The rationale put forward that it was "inherently improbable that Parliament should have refined this machinery as it did, while intending to leave in place a parallel system for obtaining evidence from abroad" (KBR (SC), [45]). The paradox picked up on by Lord Lloyd-Jones is not only applicable to the UK, it also illustrates incoherences at the international level, that a system dedicated to investigative cooperation should exist, all the while States continue to develop backchannels to circumvent it. In countries with independent judiciaries, judges should follow this lead. Indeed, only when countries will have refused extraterritorial and illegal collection of evidence will there be a true incentive to develop a functioning collaborative system.

3.2 At the intersection of multilateralism and unilateralism: crime-based sanctions

Originally reserved to foreign policy, sanctions have progressively entered the realm of transnational organised crime repression and have become a "criminal justice tool" in their own right (Moiseienko, 2024, p.18). Resorting to such practices is symptomatic of the barriers to cooperation and the failure to promote mutual trust and capacity for MLA (Herbert & Bird, 2023, p4). Crime-based sanctions are explicitly seen as an alternative or at least a compliment to MLA, as they pursue similar objectives to primary MLA given that they can result in the freezing and confiscation of assets. The CJUE has pointed to this complementarity when justifying the use of "misappropriation sanctions" against former public officials, claiming that traditional channels would lack effectiveness as they would award "enough time to transfer their assets to States having no form of cooperation with the Egyptian authorities" (Ezz et al v. Council, Case T-256/11 (Feb. 27, 2014) [66]). This EU policy can also be termed as "legal assistance sanctions" (Moiseienko and Hufnagel, 2015, p. 355). Indeed, according to Moiseienko and Hufnagel, two-types of sanctions apply directly to organised crime: the aforementioned assistance sanctions as well as crime-based sanctions which are "imposed in response to a criminal offence allegedly committed by the person targeted". Three entities are

known to actively impose sanctions on criminals: the US, the EU and the UN, the latter being the only multilateral framework in the sense that they emanate from a collective decision taken by the UN Security Council (UNSC) under article 41 of the UN Charter, and that it relies on member states for implementation. In practice, however, the UN is only a minor issuer of such sanctions. Article 24 of the UN Charter explains that the role of the UNSC is the "maintenance of international peace and security", meaning a high threshold of violence needs to be reached to gain its attention.

Applying sanctions is thus reserved to a small club of entities which have the capacity to do so either through international treaties or by *de facto* capacity awarded by a powerful position in the international economy. As such, these sanctions help to deny safe havens to criminals as their high mobility is no longer a decisive advantage. For instance, with the advent of correspondent banking, a criminal placed on the SDN list will have issues handling the proceeds wherever they are. The US's Department of the Treasury's Office of Foreign Assets Control (OFAC) has for instance made use of these prerogatives awarded by Executive Order (E.O.) 14059, which "targets persons involved in the Global Illicit Drug Trade", when targeting members of the Cartel Jalisco Nueve Generación (CJNG) involved in the trade of fentanyl.

Whereas the previous section (Section 3.1) refers to extraterritorial evidence collecting necessitating some form of encroachment of another State's sovereignty, crime-based sanctions offer the advantage of preserving, to some degree, bilateral relations. This is not to say that elevating sanctions to a systematically used tool is desirable. There would be two significant drawbacks to such a practice. Firstly, being a non-conviction-based punishment, the threshold for application is lower and a generalised application of these measures could lead to individuals having sanctions imposed onto them simply because of a lack of evidence needed for a conviction. The second issue is that despite being a criminal justice tool in practice, sanctions remain in the hands of non-judicial bodies, such as the OFAC in the US, for which national security is the main concern, rather than due process. As such, although crime-based sanctions are a useful tool which can compensate certain of the deficiencies of MLA, further *ex-ante* judicial oversight should be seen as a precondition to any further roll-out of the policy.

3.3 The Latin American model: an innovative approach with ambitions hindered by corruption, capacity and mutual trust

Latin America is characterised both by its high exposure to organised crime and by its unstable political regimes. This combination means that the region has often been at the forefront of developing legal instruments to combat the issue, yet high levels of corruption and the scarcity of binding provisions has hindered implementation. The Organisation of American States (OAS) and its creation of the Inter-American Convention Against Corruption (IACAC) was the first regional agreement of its kind, signalling a leadership role for Latin American states in the fight against corruption in the public sphere (Nagle, 2007). The manifestation of political will to combat TOC on a regional level materialised through protocols such as the Inter-American Convention Against the

Illicit Manufacturing of and Trafficking in Firearms (CIFTA). The novelty of such the project was that, rather than being a simple transposition of the UNTOC's additional protocol on regulation of arms trafficking, it catered to Latin American particularities by providing for cost-effective MLA mechanisms, limiting the impact of the lack of capacity in the region. Furthermore, the convention addressed issues of confidentiality as it attempted to garner trust between members (article 12). Despite highlighting the innovative nature of Latin American regulation, its limitations also underline the weak implementation of such measures as the text failed to provide a compliance mechanism. Scholars identify the political instability and the mass corruption as hinderances to implementation, that rises to such a high-level in certain States that political and civil society elites are reticent to implement norms that could be used against them (Nagle, 2007). High-level prosecutions linked to TOC are often conducted by the US, making use of its extraterritorial reach. It is in light of this potential for political pressure that the proposal for a Latin American and Caribbean Criminal Court Against Transnational Organised Crime (COPLA) must be read (Currie, Leon, 2018). The proposal aims to create an institution that will "investigate and prosecute the leaders and heads of criminal organisations responsible" for offences committed within its jurisdiction, which consists of Caribbean and Latin American signatories of the UNTOC. COPLA would therefore remove hinderances to MLA by creating a centralised platform that investigates and receives evidence. Such a project would provide progress in the reduction of safe havens in the region, by limiting the scope for State weakness to prevent arrest and prosecution. However, even if the project were to materialise, doubts can be raised over the political nature of such an organisation, as States such as Mexico could see high-ranking officials prosecuted (Eskauriatza, 2021). Conventions such IACAC, CIFTA and COPLA highlight the innovative stance of Latin America, all the while revealing the difficulty of such projects materialising due to issues of capacity, corruption and trust.

3.4 European Integration: closing in on the complete denial of safe havens for Transnational Organised Crime

The EU is in many ways an exception to the bilateral and informal reality of MLA as the highly integrated jurisdiction has in many aspects overcome the issue of incompatibility, trust, and capacity to develop a harmonised legal system that has considerably reduced havens within the communitarian territory. As discussed in Section 1.2, continental Europe has historically been open to MLA due to its highly mobile population, which has only grown through the process of European integration, further strengthening the case for robust judicial cooperation. Evidence of such cooperation can be traced back to 1959 and the European Convention on Mutual Assistance, but the core of the current framework for criminal matters appeared in 2000. Key instruments that constitute the innovative structure are the Schengen Information System, a database giving access to various details including identify, whereabouts and DNA (Hufnagel, 2017). Contrary to bilateral agreements, where trust is generated through diplomatic channels and is dependant on global trends, the EU court system enables judicial cooperation to continue to function by creating its own source of trust. The

particularity of the EU is that harmonisation is not only the result of domestic criminalisation, but also of supranational directives transposed into municipal law. For instance, directive 2015/849 relative to anti-money laundering provisions applied to the financial institutions called for the creation of a register of effective beneficiaries of assets that would be open to the public. The CJEU ruled that this constituted a grave interference into the fundamental right of privacy (articles 7 and 8 of the EU charter). The court exerts a limitative function, favouring confidence by ensuring that citizens will not have their rights impaired in another European jurisdiction. The ECtHR fulfils a similar role, enabling cooperation with non-member States. Strasbourg jurisprudence was used by Swiss courts to justify the carrying out of a seizure and confiscation of goods requested by Italian authorities. Despite preventive confiscation entailing an interference to the peaceful enjoyment of possessions, the Court found that the aim of authorities was both legitimate and proportional to the gravity of the case by preventing the unlawful use of possessions whose lawful origin had not been established. The ECtHR thus generates confidence between authorities by providing a common arbitration to conflicts between rights.

However, despite mechanisms created by EU conventions and trust developed by supranational courts, practical limitations persist and prevent their application. Lucas and Sánchez provide an illustration of dysfunctional procedures, as they narrate a "real story" of MLA in the EU. Common obstacles include requests simply never being completed and returned, linguistic mistakes leading to rejection and transborder interrogations failing due to technological flaws. Despite favouring direct contact through authorities, which can be done through electronic means (article 25(3) European Cybercime Convention), investigations often rely on liaison officers to verify that the request is in fact being treated, reintroducing a human element into the procedure. These remaining obstacles highlight a lack of cooperative culture between European authorities, a culture where authorities consider transnational investigations to be of prime importance.

Conclusion

A crucial mechanism to prosecute increasingly mobile organised criminals, the development of MLA has seen contrasting successes. The convergence of domestic legislation championed by multilateral institutions hides the uneven reality of MLA's extension, subject to unresolved issues of capacity and of trust. Problems concerning capacity and trust interlink to the extent that they create fear amongst developed States of confidential information leaking, whilst States necessitating investment grow frustrated by its difficulty to materialise and by intrusions into their sovereign prerogatives. Unfortunately, geopolitical trends seem to be moving towards increased distrust rather than multilateralism and cooperation. Faced with these difficulties, the US has made use of its dominant position to obtain evidence throughs its extraterritorial reach, whether this be through a long-arm approach to jurisdiction or a growing recourse to crime-based sanctions. These extraterritorial approaches, whether pursued by the US, China or others, undermine the development of an international regime.

Whereas a failure to implement stable and sustained capacity-building policies on a bilateral basis has been gradually compensated by the increasing influence of the UNODC, distrust between nations seems to be a far more deep-rooted issue. Garnering trust between States is the next crucial yet complex step to make in the promotion of further cooperation between States to reduce impunity for TOCs. If certain hinderances can only be overcome through infrastructural progress, adapting legal regimes to the transnational nature of organised crime can contribute to banishing safe havens. Both the Latin American region and the European Union seem to be paving the way for more integrated institutions, which could be the key to reducing the influence of distrust on transnational proceedings. The EU's court system that protects individual rights, although adverse effects remain, generates the confidence necessary to accepting to share sensitive information. COPLA, which contrary to the EU is a proposal emanating from States with limited capacity and trust, is another initiative designed to limit impunity through the creation of the first international criminal court for transnational crime. TOC, a tentacular phenomenon which seeks to obtain advantages by weaving its way into institutions is intrinsically linked to governments and therefore politics. Transnational proceedings are therefore highly likely to generate diplomatic tension along the way, and perhaps the creation of an international court would be a solution for prosecutions to remain unbiased.

THE DEVELOPMENT OF EQUITY UNDER THE COMMON LAW LEGAL SYSTEM: AN INTRODUCTION

AMR IBN MUNIR

SORBONNE DOCTORAL LAW REVIEW
REVUE DOCTORALE DE DROIT DE LA SORBONNE
Vol. 7 n°1

TABLE DES MATIÈRES

Résumé

Cet article traite de l'origine et de la nature de l'équité avant l'émergence du système juridique de common law. Il traite brièvement de l'émergence du système juridique de common law et de ses divers problèmes. Il explique comment l'équité était la meilleure solution de rechange au système juridique de common law. Il traite du conflit entre l'équité et la common law et de la façon dont il a pris fin. Enfin, il aborde brièvement quelques maximes équitables développées par l'équité qui sont encore utilisées aujourd'hui. Les principales conclusions de cet article sont que l'équité est un ensemble de principes qui est appliqué pour éviter l'injustice potentielle causée par l'application stricte d'une loi rigide. Elle existait en théorie et en droit même avant l'émergence de la common law. La common law est le résultat de l'application par le magistrat de vieilles coutumes et de l'émergence du stare decisis. Il avait ses propres problèmes en termes de rigidité tant dans le droit substantiel que dans la procédure. L'équité est venue comme une alternative à la common law et a été appliquée à la suite du chancelier catholique romain qui a entendu ces cas et appliqué l'équité basée sur le droit romain. En fin de compte, les tribunaux de la chancellerie ont été créés sous le chancelier, qui appliquait l'équité plutôt que la common law. Il y avait beaucoup de conflits entre les tribunaux de common law et les tribunaux de la chancellerie. Ce conflit a finalement été réglé après que le roi a décidé que l'équité devait prévaloir dans tout conflit des siècles plus tard avant de finalement avoir fusionné en une seule Cour qui a appliqué à la fois la common law et l'équité au cours du XIXe siècle. Enfin, il y a des maximes d'équité importantes qui ont été élaborées par les tribunaux de la chancellerie et qui sont encore utilisées aujourd'hui. La méthodologie utilisée pour ce travail est doctrinale.

Abstract

This paper discusses the origin and nature of equity before the emergence of the Common Law Legal System. It briefly discusses the emergence of the common law legal system and how its various problems. It discusses how equity was the best alternative to the common law legal system. It discusses the conflict between equity and common law and how it came to end. Lastly, it briefly discusses some equitable maxims developed by equity that are still in use today. The main findings of this paper are that equity is a set of principles that is applied to avoid the potential injustice caused by the strict application of a rigid law. It existed in theory and law even before the emergence of common law. Common law was the result of the magistrate's application of old customs and the emergence of *stare decisis*. It had its own problems in terms of rigidness in both substantial law and procedure. Equity came as an alternative to common law and was applied as a result of the Roman Catholic Chancellor who heard these cases and applied equity based on Roman Law. Ultimately, Courts of Chancery were developed under the Chancellor which applied equity rather than common

law. There existed a lot of conflict between both the Common Law Courts and the Chancery Courts. This conflict was finally settled after the King ruled that equity was to prevail in any conflict centuries later before ultimately having both merge into one Court which applied both common law and equity during the 19th Century. Lastly, there are some major equitable maxims that were developed by the Chancery Courts that are still in use today as well. The methodology used for this work is doctrinal.

Keywords:

Equity, Common Law, British Legal System, Civil Law, Maxims.

Introduction

This paper discusses the origin and history of equity before the emergence of the Common Law legal system; it discusses the origin of the common law legal system and the development of equity under it; it discusses the problems of common law and how these problems were overcome by equity; it discusses how there was a conflict between the Common Law Courts and the Chancery Courts which was settled with equity's victory and then the merger of both Courts centuries later; it discusses some maxims developed by equity which are still very well in use today;

6. Equity before English Common Law

Equity refers to a set of principles, a source of jurisdiction, a body of authoritative doctrines and, in some places, an institution of adjudication distinct from legal institutions.[249] It is a charitable and just principle that allows for the avoidance of the strict application of rigid law that would administer injustice rather than justice to the concerned parties in the instant case.[250] This principle has existed in various different ancient cultures in various different terminologies.[251] Equity in fact has its origin all the way back to the ancient Code of Hammurabi, which was although known for its strict adherence to principle of 'an eye for an eye and a tooth for a tooth', there were certain legal provisions incorporated within which analogously resembled equitable reliefs.[252] The concept of equity is further found in various Sumerian-Assyrio-Chaldean tablets setting forth the law as it existed a little later than the period of Hammurabi, particularly incorporating a principle of the equitable maxim, 'he who comes to equity must come with clean hands' and also the equitable right of an appeal to a higher Court.[253] These Babylon codes would be preserved and further developed by the Hebrews into the famous Mosaic Code who incorporated various moral principles derived from their religious doctrine.[254]

---

[249] Adam J. Macleod, "Why Equity Follows the Law", *Laws*, Vol. 13, No. 3, (2024), 2. <file:///C:/Users/hp/Downloads/laws-13-00003.pdf> accessed 2nd February 2024.

[250] Ibid.

[251] Margaret White, "Equity- A General Principle of Law Recognized by Civilized Nations", *Queensland University of Technology Law and Justice Journal*, Vol. 4, No. 1, (2004), 104. <https://lr.law.qut.edu.au/article/download/177/171/177-1-344-1-10-20120621.pdf> accessed 2nd February 2024.

[252] Howard L. Oleck, Historical Nature of Equity Jurisprudence, *Fordham Law Review*, Vol. 20, No. 1, (1951), 27. <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1378&context=flr> accessed 2nd February 2024.

[253] Ibid.

[254] Ibid, p. 28.

Equity is also present in Aristotle's jurisprudence as *epieikeia and epiekis* in his various treatises as a source of moral virtue which serves a specific purpose, which is to 'rectify' the law.[255] Aristotle was particularly concerned that the law was far too rigid and absolute in its administration of justice, it was much too formal and thus needed certain exceptions for certain cases where the absolute application of the law would prove to be an administration of injustice rather than justice.[256] Aristotle gives the example of a person brushing a ring on another person coming within the definition of assault as per the law, in which case, if he is charged with assault, it would not be proper administration of justice, the judge should instead endeavour to see whether such a case can come within certain exceptions where the strict application of law need not be applied.[257] Hence, he is against the literal or strict universal application of law where the law is taken even literally for even the smallest cases as is seen in the example discussed hereinabove. Thus, rather than justice being carried out, there will only be injustice and inconvenience being carried out and so, the judges should aim to make exceptions in such cases so as to make sure that justice is being carried out properly. It should also be noted that Aristotle does not mean to fill in the gaps in the law, but rather, he means that the law needs proper rectification for its certain deficiencies, that one must go beyond the codified statute or 'written law' to apply proper justice in certain cases where strict adherence to law falls short.[258] Hence, it is quite similar to the English principle of equity as we will discuss hereinbelow.

Equity was also present within ancient Roman law as *aequum/aequitas*, initially meaning level or equal.[259] It provides a basis for the analogical extension of law grounded in imaginative (if limited) empathy.[260] Hence, equity was used as a means of moderating the law and applying natural justice to reach a fair and just conclusion to cases.[261]

Under ancient Chinese jurisprudence, equity existed under the principle of *qingli*, which refers to compassion.[262] Similar to its western counterpart, any positive rule that was inconsistent would be

---

[255] For a comprehensive discussion of Aristotle's exposition of equity, see: Roger A. Shiner, Aristotle's Theory of Equity, *Loyala of Los Angelos Law Review*, Vol. 27, No. 4, (6-1-1994), 1251. <https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1859&context=llr > accessed 2 February 2024.

[256] Ibid.

[257] Ibid.

[258] Ibid, p. 1255.

[259] Stephen Humphrey, "Equity before Equity", *Modern Law Review*, Vol. 86, No. 1, (2023), 86. <https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12750> accessed 2nd February 2024.

[260] Ibid.

[261] Macleod, Equity Follows, 2.

[262] See: Xi Lin, "*Equity in the Chinese Law: Its Origin and Transformations*", (PHD Thesis: The London School of Economics, 2008), 10. <https://etheses.lse.ac.uk/2974/1/U615926.pdf> accessed 2nd February 2024.

rejected in favour of it.[263] Under ancient Hindu Jurisprudence, equity can be traced within the *Hindu* law of *Dharma*, which has multiple definitions which include natural law, morality, justice, virtue, moral law, duty among others.[264]

Under Islamic Law, there is a debate on whether *istihsan* is the Islamic equivalent of equity.[265] In fact, it has even been referred to as "juristic equity".[266] It is a subsidiary source of Islamic law and a principle which was developed by the *Hanafis* to remove the rigidity of law in certain situations.[267] It is designed to make up the defect in law owing to its generality or to remove its rigidity.[268] According to Ahmed Hasan, there are situations in an ever evolving human society which calls for a departure from the strict application of the law and thus, in such a case, the jurist should be allowed leeway to depart from the established rules of law and apply another principle keeping in mind public interest and human good.[269] Hence, *istihsan* becomes a useful principle for legislating on fresh principles as it can be utilized for situations for which one cannot find any principle or rule from the classical legal treatises.[270] This exposition seems similar to the expositions of equity as discussed hereinabove.

Hence, we can see that the precept of equity has existed long ago in theory or as a principle of law and it more or less refers to the principle of departing from the strict application of a particular law in certain cases where it would cause injustice rather than justice and in order to combat this and administer proper justice in such cases, one must apply a principle which is fair, just and will administer justice in the instant case.

7. Origin and Development under Anglo Jurisprudence

To understand equity, it is important to discuss common law first. Common law can be described as the judge-made law of England based on custom although it is disputed whether judges make law or

---

[263] Ibid.

[264] Sunil Sondhi, "Aspects of Dharma Ethics Law and Action in Indian Tradition". <https://hal.science/hal-04188649/document> accessed 2nd February 2024.

[265] John Makidsi, "Legal Logic and Equity in Islamic Law", *The American Journal of Comparative Law*, Vol. 33, No. 1, (1985), 67. <https://www.jstor.org/stable/840118> accessed 2nd February 2024.

[266] Abdur Rahim, "*The Principles of Muhammmadan Jurisprudence According to the Hanafi, Maliki, Shaf'i and Hanbali Schools*", (Luzac & Co., 1911), pp. 163-166.

[267] For a comprehensive discussion on the principle of *Istihsan*, see: Ahmed Hasan, "The Principle of Istihsan in Islamic Jurisprudence", *Islamic Studies*, Vol. 16, No. 4 (1977), 347. <https://www.jstor.org/stable/20847051> accessed 2nd February 2024.

[268] Ibid.

[269] Ibid, p. 360.

[270] Ibid.

discover it.[271] After the Norman Conquest in 1066, the first Norman King, William the Conqueror set up the *Curia Regis* (the King's Court) and appointed his own Judges. These Judges were sent to other towns as well to decide cases that arose there. Overtime in the era of Henry II, the visits became more and more regular and the Judges would travel all over the country from London to decide cases. These judges would decide cases by local customs or old Anglo-Saxon laws. It is believed, however, that the judges upon their return to London would discuss the cases they decided and would discuss the best customs to be used by all of them should they encounter similar cases later on. This had the intended effect of the law of England becoming more uniform or 'common'. This is where the phrase "common law" seemed to have developed. The traveling magistrates started the practice of deciding similar cases similarly and hence the doctrine of *stare decisis* (let us stand by things decided) took birth which evolved into the concept of judicial precedents and became the hallmark of so many legal systems today.[272]

We have already discussed what common law is and how it developed. Now let us discuss the problems that it caused and how equity emerged as the answer to fill in the gaps in common law. Common law was much too rigid in the early years. Only certain types of cases were recognized and could be brought to the common law courts. A person could lose his case by a simple error in the formalities! The only remedy common law could give to people was damages, which could not always be the appropriate remedy for each and every case. Suppose, A trespasses into B's land and builds something there, should B approach the common law court, the only remedy the common law court could give was ordering A to pay B in damages, which would be very unsatisfactory for B. B would rather have the building that A built on his land to be removed rather than be paid in damages. This rigidness was the primary cause for concern among the common folk of England who wished for far better justice than simply to be paid in damages each and every time. Similarly, a case could only be registered if a certain amount of money was paid to court's staff first. In some cases, the money to be recovered was less than the amount to be paid for the case to be registered. In such case the poor claimant had no choice but to forgo registration of his case. When the case would be registered the common law court had no power to force the respondent to appear before it. It was a common excuse for a respondent to say that he was on a crusade and could not appear before the court. Bribery and corruption were common. A litigant bringing the greatest number of witnesses would win the case and such witnesses were available outside the court and would go with any litigant for money. In addition, the common law court was using Latin as the language of the court and procedure and the common litigants would not know about the conduct of the proceedings in the

---

[271] For a comprehensive discussion on this debate, see: Muhammad Munir, "Are Judges the Makers or Discoverers of the Law? Theories of Adjudication and Stare Decisis with Special Reference to Case Law in Pakistan", *Annual Journal of International Islamic University Islamabad*, Vol. 21, (2013), pp. 7-40. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1792413> accessed 2nd February 2024.

[272] For more information on the history and development of the English Common Law legal system, see: George Burton Adams, "The Origin of the Common Law", *The Yale Law Journal*, Vol. 34, No. 2 (1924), pp. 115-128. <https://www.jstor.org/stable/788661> accessed 2nd February 2024.

court. Common people were sick of this system and they started approaching the King through application about their legal issues. The King used to be a busy man and would simply pass on such an application to his Chancellor who was the most religious person and was considered King's link to God and "Keeper of the King's Conscience".[273] He would quickly decide such cases according to equity (literally fairness). While it literally means fairness, it has been defined as "in its broadest sense, equity is fairness. As a legal system, it is a body of law that addresses concerns that fall outside the jurisdiction of common law. Equity is also used to describe the money value of property in excess of claims, liens, or mortgages on the property."[274] Hence, a system that emerged by following fairness rather than the strict and rigid tenants of the common law. Unlike the common law courts, this informal but very quick adjudication system had no formalities and was without technicalities. It started the practice of sending summons to the respondent forcing him to appear before it. It used English as the language for adjudication. Thus, the court was doing equity, justice, and fairness and was known as the court of equity. It is on this basis that the system of equity evolved. The Chancellor would decide cases on the principles of natural justice, fairness and good conscience rather than the customs and precedents that were decided previously. He was a churchman who was familiar with Roman Law.[275] Hence, we can clearly see that the Chancellor applied Roman equitable principles in the petitions that he heard.[276] He was also prepared to look beyond legal documents which were considered legally binding by the common law courts, and to take account of what the parties intended to do.[277] He also introduced new procedures such as "subpoenas"[278] and developed new remedies such as injunctions, specific performance, rescission and rectification. An injunction is an order of a court to perform or not to perform an act, specific performance is an order of the court to carry out the contract as originally agreed between the parties, rescission is the process of returning the parties as far as possible to their original positions before performing the contract, whereas rectification is the altering or rectifying a mistake in a document as the mistake does not reflect the true intention of the parties. Overtime equitable maxims were also developed as well which are also very well in use today. One can only be astonished and be at awe at the legal mind of the Chancellor for developing all these in order to tackle the problems caused by common law. Eventually a Court of Chancery headed under the Chancellor was established which

---

[273] Jacqueline Martin, *The English Legal System* (Italy: Hodder Education, 8th ed. 2016), 18. See also, Thomas O. Main, Tradition Equity and Contemporary Procedure, *Washington Law Review*, Vol. 78, (2003), 441. <https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1725&context=facpub> accessed 2nd February 2024.

[274] *West's Encyclopedia of American Law*, (Thomson Gale, 2nd ed. 2005), 199.

[275] Thomas O. Main, Tradition Equity and Contemporary Procedure, *Washington Law Review*, Vol. 78, (2003), 441. <https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1725&context=facpub> accessed 2nd February 2024.

[276] Edward D. Re, The Roman Contribution to the Common Law, *Fordham Law Review*, Vol. 29, No. 3, (1961), 462. <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1673&context=flr> accessed 7th February 2024.

[277] Ibid.

[278] An order issued to a witness to attend court lest he risk a penalty by the Court.

operated under the rules of fairness/equity. The Court of Chancery was originally an administrative body under the Lord Chancellor which became a largely judicial body in the 14th century which further developed the doctrine of equity.[279] While it was not an ecclesiastical court, its presiding Officer, the Chancellor was one, he had knowledge of Roman and thus applied it in different cases.[280] In fact, the Court of Chancery was also called "Backbone to the Roman" as the equitable principles developed under Roman civil law largely entered to the English legal system from here.[281] Of course, it was not always uphill from here. Another major problem occurred which was a conflict between the common law court and the Court of Chancery. The common law court would decide a matter in one way and the same would be decided differently by the Court of Chancery. These two Courts would clash again and again. A person who had his case decided not in his favour by the common law court would simply go to the Court of Chancery which would decide the matter in his favour. Hence the legal system was in peril at that time. The controversy was eventually resolved in the famous *Earl of Oxford's case*[282]. The King, James I on the advice of the then Attorney General Sir Francis Bacon ruled that in a case where there is a conflict between equity and common law, equity shall prevail. This was a major victory for equity. Hence, the position of equity being the more dominant force against common law prevailed for the next two centuries until the passing of the Judicature Acts of 1873-1875, which merged the common law court with the Court of Chancery and its jurisdiction was transferred to the Chancery Division of the High Court. Hence, equity and common law merged, no longer would there be any conflict or other problems occurring between the two. And naturally, all of this not just had an impact in just England but also, its various colonies all of which included British India as well.

8. Equitable Maxims

What exactly is a maxim? It has been defined as "a broad statement of principle, the truth and reasonableness of which are self-evident. A rule of equity, the system of justice that complements the common law."[283] It has also been defined as "an established principle or proposition. A principle of law universally admitted, as being a correct statement of the law, or as agreeable to natural reason. Coke writs that "a maxime is a proposition to be of all men confessed and granted without proof,

---

[279] Main, Equity, pp. 442-443. See also: <https://www.judiciary.uk/courts-and-tribunals/business-and-property-courts/chancery-division/the-work-of-the-chancery-division/introduction-to-the-chancery-division/#:~:text=The%20Court%20of%20Chancery%20was,developed%20the%20doctrine%20of%20equity.> accessed December 10, 2022.

[280] D. Re, Roman Contribution, 462.

[281] Ibid.

[282] (1615) 21 ER 485.

[283] *West's Encyclopedia of American Law*, (Thomson Gale, 2nd ed. 2005), 466.

argument, or discourse."[284] Hence, we can conclude that a maxim can be seen as a principle that is to followed by all. The system of equity naturally developed its own maxims which it endorsed and followed. The courts generally justify their decisions and base basic principles of equity by these maxims which in turn have guided the development of equity. The major equitable maxims are as follows:

No wrong without a remedy

Wherever a wrong has been committed, equity will always provide a remedy. It is from here that the principle of always providing remedy for anyone whose legal right has been infringed. Hence, equity will always provide where a legal wrong has been committed, not where a moral wrong is committed. It is also thanks to this maxim that the development of new equitable remedies is possible.

Equity acts in personam

This maxim refers to the fact that equity issued its decrees against a person himself. If the person did not comply, he was liable for imprisonment. Hence, judicial obedience was evolved through this maxim.

Equity acts on the conscience

Equity looks at the conscience of the parties. Equity does not give justice to anyone who does not come with a clean conscience, in other words, someone who has malicious intentions should not come to equity.

Equity aids the vigilant, not the indolent/Delay Defeats equity

Equity does not provide aid to those who were far too late in seeking equitable remedies. If a person took too much time in his claim, then he could not be reasonably provided with remedies as this would be unfair to the other party. This was first applied in *Leaf v International Galleries*[285]. In this case, a plaintiff bought a painting which both parties believed to be painted by Constable. It was found out later on that it was not in fact a painting by Constable. The plaintiff issued a claim, albeit five years later. Denning LJ. ruled that the right to rescind the contract cannot be enforced as there was a delay of five years in between buying the painting and discovering that it was not a painting by Constable.

Equity looks to the intention and not the form

This maxim simply means that equity is to look at the intention of the parties who were engaged in a contract or anything rather than the contract or any other document itself. Equity is to ascertain what

---

[284] Henry Campbell Black, *Black's Law Dictionary*, (St. Paul, Minn. West Publishing Co., 2nd ed. 1910), 767.

[285] [1950] 2 KB 86.

the original intentions of the parties at the time of agreement rather than what has been agreed upon, especially if the agreement itself suffered from mistakes. In the case of *Berry v. Berry*[286], a deed was held to have been altered by a contract. Under common law, a deed could only be altered by another deed, but under equity, it was decided that as the parties had originally intended to alter the deed, it would be fairer to look at the intention of the parties rather than the fact that the parties had gotten the formalities wrong.

He who comes to equity must come with clean hands

This is similar to the maxim *equity acts on conscience*. Anyone who has acted unfairly or with ulterior motives in mind will not be granted any equitable relief. In the case of *D & C Builders Ltd v Rees*[287], Mr. and Mrs. Rees refused to pay full payment to a construction firm that had done work for them. The Rees had paid 250 pounds in advance out of the total bill of 732 pounds. When the firm asked for the remaining 482 pounds back, the Rees who knew that the workers were in financial difficulty and needed money urgently refused to pay the whole amount, claiming that the work had not been done properly and they would only pay 300 pounds. The firm accepted it reluctantly at first but later on sued the Rees for the remaining amount. Lord Denning held that the doctrine of estoppel (an equitable doctrine in which the courts can declare that the plaintiffs are prevented from asking for the rest of the amount) will not be applied here as the Rees family who knew that the workers were in financial difficulty and took unfair advantage of it did not come with clean hands.

He who seeks equity must do equity

Again, a similar maxim to the ones mentioned above, except in this case the petitioner's present actions and conduct will be taken into account.

Where the equities are equal, the earlier in time prevails

Where the rights of the parties are equal both in worth or value, the one who comes first shall prevail. Hence, this follows the concept of "first come, first serve".

Equity follows the law

Equity will follow common law unless there is a good reason to the contrary. Where the law is not providing proper justice to the parties, equity is there to fill in the gaps and provide proper justice.

Equity looks at that to be done which ought to be done

Equity looks at the obligations that should have been fulfilled rather then what the party did as thought best. Equity will look and treat any intention to fulfill an obligation as something has already been fulfilled.

---

[286] [1929] 2 KB 316 = 98 LJKB 748.

[287] [1965] 3 All ER 837.

Equity imputes an intent to fulfill an obligation

Again, similar to the one above, equity will presume an act done by a man as a just and right act.

Equity will not assist a volunteer

Equity shall not assist anyone who gives no consideration.

These are the major maxims of equity that have been used and developed by the courts.

Conclusion

Hence from the discussion hereinabove, we can conclude that equity refers to the set of principles that allow for the avoidance of the strict application of a rigid law so as to make sure that justice rather than injustice is administered in the instant case. It has its origin in various different cultures in some form as a theory or a legal principle. It stems its origin all the way back from the Code of Hammurabi and other Babylonian tribes to the Hebrew tribe's addition of moral principles derived from their religious doctrines to Aristotle's exposition of *epieikeia and epiekis*, where he surmises equity is to be used for the 'rectification' of law rather, where the law is too strict and absolute and its literal application would result in injustice rather than justice. The Romans incorporated the principles of equity under the precept of *aequum/aequitas*, which means equality. The Romans further developed equity in the form various legal principles under their codified law. Equity was also present under ancient Chinese jurisprudence as *qingli*, which refers to compassion and was also present under the ancient Hindu jurisprudence of *dharma*, which is the Hindu law of righteousness and has also been referred to natural law, morality, moral law, duty among others. Under Islamic Law, there is a debate that the doctrine of *istihsan* is the Islamic counterpart of equity, although there are certain similarities between both. The English Common Law was developed after the Norman King, William the Conqueror sent a lot of his magistrates to various different towns to decide cases. These judges decided cases based on old Anglo-Saxon custom and it is believed that on their return to England, they all together decided on the best customs to apply to particular cases. This was a means of an effort to make the English law more uniform. Ultimately, it let to the application and development of the doctrine of *stare decisis* (similar cases are to decided similarly). The legal system suffered from a lot of rigidness. The Common Law courts strictly applied to the law which caused a lot of inconvenience to parties, it suffered from a distinctive lack of remedies. In fact, the only remedy common law had was to give damages to the victim party. It suffered from procedural rigidness as well. It had no power to summon parties before them. If someone could not deposit the required amount for the registration of his case, then his case would not be registered. The Common Law courts also exclusively used Latin instead of English which caused a lot of communication problems. Due to this a lot of parties appealed to the King. The King, being a busy man handed such cases to his Chancellor, who was a Roman catholic and had knowledge of roman law. He developed many different equitable principles and new procedures such as subpoenas and summons to dispense

with speedy and proper justice. Ultimately, a Court of Chancery under the Chancellor was constituted. The Chancery Court applied the principle of equity as compared to the Common Law courts which applied the Common Law. Then arose a long conflict between the Chancery Courts and Common Law Courts over jurisdictional issues. One person could lose his case at one Court and win his case at the other Court. This conflict was eventually settled centuries later where the King decided that in a conflict between equity and common law, the former was to prevail. During the 19th century, both the Chancery Courts and the Common Law Courts as a result of the Judicature Act, 1873-1875 and thus there was one Court which was to apply both common law and equity. There are many different equitable maxims that were developed by the Courts that are still in use today, namely: No wrong without a remedy, equity acts in *personam*, equity acts on the conscience, equity aids the vigilant, not the indolent/Delay Defeats equity, equity looks to the intention and not the form, he who comes to equity must come with clean hands, he who seeks equity must do equity, where the equities are equal, the earlier in time prevails, equity follows the law, equity looks at that to be done which ought to be done, equity imputes an intent to fulfill an obligation, equity will not assist a volunteer.