

Personal Data Ownership: Legal Analysis and a Proposed Model

Ghaleb Neymer ALAdwan* 

Department of Private Law, School of Law, The University of Jordan, Amman, Jordan

Received: 09/11/2025
Revised: 21/12/2025
Accepted: 19/04/2026
Publish online: 4/6/2026

* Corresponding author:
ghalibaladwan@outlook.com

Citation: ALAdwan, G. N. (2026).
Personal Data Ownership: Legal
Analysis and a Proposed
Model. *Dirasat: Shari'a and Law
Sciences*, 13580.
<https://doi.org/10.35516/Law.2026.13580>

Abstract

Objective: This paper explores the ownership model for personal data protection in comparison to competing models, assesses the legal grounds for applying property rights to personal data, and suggests a regulatory framework for individual ownership.

Methods: This study utilizes a doctrinal methodology to analyze the concepts of ownership and property. It compares the model of ownership with the main frameworks for personal data protection, examines the legal basis for applying ownership rights to personal data, and proposes a regulatory model for personal data ownership.

Results: The findings indicate that the ownership model may offer stronger protection for personal data compared to other models, such as fiduciary, human rights, and self-determination models. Consequently, this study suggests adopting a property model akin to that of intellectual property, which differentiates between moral rights and economic rights.

Conclusion: Protecting privacy and personal data requires recognizing individuals' property rights over their information. Ownership appears to provide better protection for personal data compared to other models. However, existing Personal Data Protection Laws (PDPLs) do not include any clear resolution regarding the debate over personal data ownership. Identifying this gap, this paper argues that property rights are a natural right and that the concept of property includes both tangible and intangible assets. Therefore, it proposes a regulatory model for personal data ownership. Similar to intellectual property, personal data encompasses both moral and economic rights.

Keywords: Personal data, Jordanian personal data protection law of 2023, GDPR, CCPA, privacy.

ملكية البيانات الشخصية: دراسة تحليلية مقارنة ونموذج بديل للملكية

غالب نمر العدوان*

قسم القانون الخاص، كلية الحقوق، الجامعة الأردنية، الأردن

ملخص

الأهداف: تهدف هذه الدراسة إلى بحث نموذج الملكية كنموذج لحماية البيانات الشخصية بالمقارنة مع النماذج المنافسة، والنظر في الأسس القانونية التي يُمكن الاستناد إليها لتطبيق حق الملكية على البيانات الشخصية. واقتراح نموذج قانوني للملكية في البيانات الشخصية.

المنهجية: تم إجراء الدراسة باستخدام المنهج الوصفي التحليلي خلال تحليل مفهوم حق الملكية والملكية. بالإضافة دراسة نموذج الملكية في حماية البيانات الشخصية مع المقارنة بالنماذج الرئيسية المُقابلة، بالإضافة إلى تحليل الأساس القانوني لتطبيق حق الملكية على البيانات الشخصية واقتراح نموذج لحق الملكية حولها.

النتائج: توصلت هذه الدراسة إلى عدد من النتائج، أهمها أن تطبيق نموذج حق الملكية الفردية في البيانات الشخصية قد يساهم في توفير حماية أفضل للبيانات الشخصية من النماذج المقارنة كنموذج حقوق الإنسان وأمناء البيانات، وتقرير المصير المعلوماتي. وعليه، قدمت الدراسة نموذجاً لحق الملكية حول البيانات مشابهاً لنموذج الملكية الفكرية، وذلك من خلال تقسيمها إلى حقوق معنوية ومادية.

الخلاصة: تتطلب حماية الخصوصية والبيانات الشخصية الاعتراف بحق الملكية على هذه البيانات حيث إن نموذج الملكية يُقدم حماية للبيانات أكثر من النماذج الأخرى. ومع ذلك، لم تتضمن قوانين حماية البيانات الشخصية معالجة واضحة لهذه المسألة. وعلى ضوءه، تجادل هذه الدراسة بأن حق الملكية هو من الحقوق الطبيعية، وأن مفهوم الملكية يشمل كل من ملكية الأشياء المادية والمعنوية. وعليه تقترح هذه الدراسة نموذجاً للملكية حول البيانات مقارباً لمفهوم الملكية الفكرية حيث ينقسم إلى حقوق مادية (اقتصادية) ومعنوية.

الكلمات الدالة: قانون حماية البيانات الشخصية الأردني لسنة 2023، اللائحة الأوروبية العامة لحماية البيانات الشخصية، قانون كاليفورنيا لحماية بيانات المستهلك، الخصوصية.



© 2027 DSR Publishers/ The University of Jordan.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license <https://creativecommons.org/licenses/by-nc/4.0/>

1. Introduction:

In the contemporary era of digital transformation and a data-driven market, protecting personal data may be the most significant requirement for protecting the right to privacy. The right of privacy is among the essential human rights, which is mentioned in the Universal Declaration of Human Rights, Article 12: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence...” and is defined simply as “the right to be let alone” (Warren & Brandeis, 1890 as cited by Zimmerman, 1983). Even though some authors differentiate the right of privacy from the right of personal data protection, that does not change the fact that personal data protection is the most essential requirement to protect the right of privacy.

Given the foregoing, personal data protection requires a broad and flexible legal framework that protects personal data without hindering digital transformation or economic progress. Thereby, many legislators have issued the legal framework of personal data protection to protect individuals' data privacy and, at the same time, regulate the processing of this data by both public and private entities in a manner that enhances economic and social progress (Regulation (EU) 2016/679 [GDPR], 2016, Recital 2,4).

There is no doubt that Personal data protection laws are among the core pieces of legislation for safeguarding privacy and have emerged to emphasize and preserve this right by protecting our personal data. However, relying on personal data protection laws to safeguard our privacy in the age of big data may be insufficient. PDPLs are based on the idea that protecting personal data is a fundamental right, but by examining these laws, we can notice that Jordanian PDPL, GDPR, and CCPA are full of exceptions that allow data controllers to process data without the consent of the data subject (Thouvenin, 2021). This gap in personal data protection intensified the author's desire to seek an alternative model.

This approach was built while considering that the relationship between those two rights has long been recognized as integral (Bell and parchomovsky, 2019). Nevertheless, Legislators seem to have overlooked the lack of explicit regulation of the right to property over personal data (Purtova, 2010). Therefore, the idea of ownership might be the most rational and safe approach to be adopted as a personal data protection model. However, PDP regulatory systems are focused on how to protect personal data from unlawful or illegitimate processing or use by controllers and their proxies, but not on allocating the ownership of it to individuals (from whom the data originates).

Some authors argue that these regulatory frameworks grant individuals property rights in some form (Bambauer, 2024; Hazel, 2020). Yet this claim does not appear to align with the regulatory approach in the addressed PDPLs. Thus, further research is needed on the ownership of personal data and the potential that the ownership model has compared to its rivals.

1.1 Research objects:

The study investigates the concept of ownership and property under the civil law conception and how it could be applied to personal data as a model of protection and control in comparison with the primary models in this area. Also, examining and assessing the PDPL regulatory status quo regarding ownership rights. Moreover, it aims to examine whether there is a legal basis for applying the ownership right over personal data. And if so, what model of property could be used in this case?

For these purposes, the research will analyze the concept of personal data ownership under personal data protection laws. It will further address the main models of personal data protection and whether the notion of property rights acknowledged by civil Law applies to the current regulatory approach of personal data protection. Finally, this paper will examine the legal basis for recognizing whether individuals can own personal data and propose a regulatory model for ownership.

1.2 Methodology:

This research employs a doctrinal methodology to address the theoretical gap between the right of ownership and the personal data protection system by following the following steps:

- Conceptual foundation: by conducting a primary analysis of the concepts of ownership rights, personal data, and property.
- Executing a comparative modeling approach: through addressing and evaluating ownership and the primary models for personal data protection.
- PDPL regulatory status quo assessment: by analyzing and comparing the positions of the Jordanian Personal Data

Protection Law, the General Data Protection Regulation of 2018, and the California Consumer Privacy Act of 2018 regarding ownership of personal data, and, where applicable, examining relevant case law.

- Normative modeling: by investigating a legal basis for ownership rights over personal data within the Jordanian Civil Code's property rights framework, and proposing a viable regulatory personal data protection model through personal data ownership.
- This research employs the comparative methodology only regarding the investigation of data subject rights, and the reason behind choosing GDPR and CCPA as the subjects of comparison is that GDPR, considered a comprehensive PDPL model, serves as the global standard for a rights-oriented approach. On the other hand, CCPA represents the market-oriented model, providing a crucial comparison perspective in this area.

2. Personal Data and the right of ownership, matters of interpretation:

2.1 What is personal data?

2.1.1 The difference between Data and Personal data:

Understanding the concept of data is a significant step toward discussing ownership rights over it. While personal data plays a major role in digital transformation and is considered the most valuable and crucial asset in the digital economy, not all Data should be treated as personal data. In fact, data as a concept is more comprehensive than personal data. Given all of that, personal data is only one of the different types of data (Offor, 2020). Nevertheless, the boundary line between the two concepts is vague and unstable. Typically, what is considered non-personal data today may be regarded as personal data in the future. Such a change could result from technological development and other factors. (Wendehorst, 2022). Notwithstanding, drawing borders between the two concepts is of paramount importance (Finck and Pallas., 2020). Therefore, a disclaimer should be made in this context, since this study focuses only on personal data ownership; other types of data, such as public or private entities' data, are out of the scope of this research.

2.1.2. Personal data legal definition:

According to the ART2 of Jordanian PDPL No. 24 of 2023, personal data is defined as “Any data or information related to a natural person that directly or indirectly identifies them, regardless of its source or form. This includes data concerning the individual, their family status, or their location, which is similar to the definition in Article 4 of the GDPR. California Consumer Privacy Act of 2018 took the same direction as both. It defines personal information in ART 1798.140 \ V as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household...” (California Consumer Privacy act., 2018).

Personal data could as well be defined as “data that is an attribute of an individual” (Parkinson, 2018), it could be also defined as “data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practicable matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual” (Simon and Graham. 2017. As cited in Parkinson, 2018).

Based on the above, personal data refers to information that can be attributed to a specific individual or that could identify them, directly or indirectly. So, in contrary, non-personal data is data that is not related to a particular person or an indeterminate individual.

2.2. What is the right of ownership?

The theory of property has long been a subject of debate, and property regimes are various and somewhat complicated (Finnis, 2011). And the concept of property in the civil law regime may evidently be different from what it is in the common law, even though the differences have lately been superficial and barely considerable (Pierre, 1997.). Nevertheless, in the subsequent analysis, we will focus on the concept of property recognized by civil law.

2.2.1. The main characteristics of property rights:

The right of property (ownership) is defined under the Jordanian Civil Law No. 43 of 1976 as: “The authority of the owner to dispose absolutely of his property itself (the corpus), usufruct and exploitation.” In accordance with this article, property right give their holder (which is the data subject in our case) the authority to leverage their property in multiple

ways (selling, leasing, transferring, or by any means within the limits of the Law's provisions).

A similar definition was provided by the French legislator in the French civil law: "Ownership is the right to enjoy and dispose of things in the most absolute manner, provided they are not used in a way prohibited by statutes or regulations". Akin to the Jordanian definition of ownership right, it is not absolute either, as the French legislator stipulated that "No one may be compelled to yield his ownership, unless for public purposes and for a fair and previous indemnity." (French Civil Law, 1804).

In jurisprudence, some authors distinguish between property and ownership rights. According to this view, property is broader than ownership; ownership is the core of property, understood as the authority to be in exclusive charge of a specific thing (Katz, 2017). It is also defined by the English jurist "Austen" as "the right to use something and the power to exclude others from its use" (Rees, 2014).

A disclaimer must be made here: this research examines property rights primarily under the provisions of the Jordanian Civil Code of 1976, which means it investigates this right from a civil law perspective. Thus, it won't be restricted by the principle of the "numerous clauses" doctrine, which implies that property rights are specified with only a pre-determined list of rights. Other types of rights that may appear related to ownership rights shall not be considered if they do not meet the criteria set forth (Weir, 2015).

2.2.2. The aspects of ownership rights:

Based on the above, property rights have two aspects:

- A) The positive aspect (the right to use the property in any manner, within the limits of law).
- B) The passive aspect (the right to exclude or prevent others from using property).

If one of the two aspects is absent, we cannot confidently conclude that we are dealing with the right of property.

3. Understanding the concept of property.

Before addressing the positions of PDPL's regulatory systems, we must first examine the concept of what the civil code considers property, taking into account the legal nature of personal data and whether it is subject to ownership rights under the law.

3.1 Drawing boundaries of the property concept:

Property, as a legal concept, has evolved. Property was once understood to include only tangible things, such as books, tables, and, primarily, land. However, the property concept in modern comprehension includes intangible things and other sorts, like intellectual property (Esmaeili & Grigg, 2016). Property, as a term, may indicate both the goods themselves and the goods that are subject to property rights (Zambon, 2019). For this study, we will use the term of property to indicate the good itself, which is personal data in our case, away from the legal long debate.

3.2 Property according to Jordanian Civil Code No. 43 of 1976:

To provide a comprehensive understanding of the concept of property under the Jordanian civil code, we need to examine the legal texts that regulate and define this right. According to Article 53, "property is every corporeal thing or right that has a financial value in legal transactions". And Article 54 states that: "everything that could be possessed physically or non-physically and leveraged from it in a legitimate manner and not excluded from dealing by nature or by the rule law may be subject to financial rights". Article 55 explains the things that could not be possessed by nature. It says, "things that excluded, by nature, from dealing are these that no one can monopolize their possession, and the things that are out of dealing by the rule of law are things that law prohibit them from being subject to financial rights.

Based on this statutory foundation, Jordanian law adopts a broad and somewhat flexible definition of property. Articles 53, 54, and 55 interpretation indicates that the property concept applies to everything, whether tangible or intangible, which can be considered as property unless it cannot be possessed in an exclusive manner or it is prohibited from dealing by the rule of Law.

4. Why does ownership matter?

Ownership rights over personal data have always been controversial and a subject of ongoing debate (Bell and Parchomovsky, 2019). Traditionally, Privacy was believed, for a long time, to be nothing but an extension of property rights

(Seipp, 1981.). Today, personal data is considered a central subject of privacy rights due to technological, market, and social developments. If personal data cannot be protected, there is no privacy anymore. Back to history, the right of privacy was protected only under the scope of property rights (Seipp, 1981.). tracing ownership of personal data back to data subjects, will be a crucial step to make their right to privacy more applicable and effective in practice, as individuals will eventually have the right to exclude others from using their data. It will enhance their position vis-à-vis companies and data collectors (Amstutz, 2018, as cited in Thouvenin and Tamò-Larrieux, 2021).

Nevertheless, Personal data is considered, from an economic perspective, a valuable asset. On one hand, free access to personal data will enable data controllers and merchants to use it in a way that enhances their sales capabilities. If they acquired knowledge of an individual's preferences, they would use this information to influence their shopping behavior in their own interests. In other words, businesses rely on the flow and accessibility of personal data (Paskaleva, 2024). On the other hand, depriving businesses of the ability to aggregate personal data will prevent them from using it for advertising and marketing purposes (Acquisti et al., 2016). Allocating ownership of personal data to individuals will strengthen their position as data controllers vis-à-vis businesses and other entities, including public entities. Thus, it might be a negative issue for companies. However, this argument appears somewhat one-sided; stricter data protection may have both positive and negative consequences. For example, protecting and regulating personal data may appear to affect marketing and advertising, leading to severe adverse economic consequences. However, studies show that it may negatively affect a subset of ads, not all of them (Goldfarb and Tucker 2011, as cited in Acquisti et al., 2016). Moreover, the propertisation of personal data may facilitate the data market by improving data quality, thereby positively affecting transaction efficiency (Purtova, 2011).

Furthermore, control over privacy and personal data was consistently recognized and achieved through property rights in personal data (Solove, 2001). By attributing the ownership of this data to individuals, they will have greater control over it, as reflected in the rights outlined in the PDPLS (Janeček, V., 2018), which provide an adequate legal mechanism for protecting their privacy (Litman, 2000; Purtova, 2011). In addition, it would enhance their ability to protect their own data by enabling them to identify the party that breached their personal data and who is responsible for it, and to hold that party liable for any action that adversely affects the personal data (Purtova, 2010 and Bambauer, 2024).

Moreover, granting ownership right over Personal data will help in organizing the data market: the parties involved in this field. It will also pave the way for legislators, privacy policy, and guideline developers to establish a clear approach to personal data protection (Rees, 2014). However, one of the main arguments against ownership is that it would incentivize vulnerable people to sell their data, thereby exacerbating existing inequities (Viljoen, Salomé. 2020, as cited in The World Bank, 2021). While this might be true, according to the status quo, entities from both private and public sectors are gaining tremendous profits by using the data of individuals via transferring, marketing, and etc.), thus allowing enterprises to achieve profits by commercialising personal data while preventing the "owners" of their data from such an act is really what exacerbates the inequities. Besides, the right of property is more about protecting and excluding third parties from using personal data than alienating it. Since the idea of an absolute free market in the context of every sort of product or goods is just a myth. Regulatory restrictions always exist (Bergelson, 2003 and Purtova 2010)

Considering the foregoing, some argue that the ownership model might create practical challenges to the current personal data status quo. For instance, when some authorities or entities force you to provide or transfer your data, this might indicate one of two: you do not own it, or you are not the only one. The idea of common ownership might be, to some extent, logically and legally improper, because fostering the commons as the concept of property in personal data will raise many questions about the legal foundation of it in terms of "personal" data, the authorities of the owners, their roles and responsibilities regarding personal data, etc. (di Robilant, 2013). Accordingly, the second choice is ruled out. But what about the first one?

In terms of personal data, authors argue that it is hard, if not impossible, to maneuver the tactics that data collectors use (Litman, 2000). Contemporary ecosystems and lifestyles are pushing us, in some ways, to provide our data not only to the public sector (justified by public interest purposes) but also to the private sector. In the current personal data ecosystem, our data does not always reach the controllers voluntarily; rather, unwillingly. Moreover, it is being shared between different parties in different situations and considerations (Al-Khouri, 2012; D'Hauwers & Vandercruysse, 2025). Thus, assigning

ownership of personal data to individuals do not align with the current status quo; such a shift will require significant changes to this ecosystem.

In fact, this argument is prompting a shift toward personal data ownership by shedding light on the significant consequences of current approaches to personal data. Therefore, to enhance individuals' privacy and personal data protection, substantial modifications are needed (Shehu and Shehu, 2023). Personal data ownership might be the only solution that can solve the problems and fill the gaps that the rivalry models cannot.

5. Is there an alternative model of protection other than ownership?

Given that protecting data's privacy is the main goal behind this research. Examining other control models appears to be substantial. The main models in this context are the human rights model, the harm-based model, the data fiduciary model, and the informational self-determination model.

5.1 Human rights model:

This model is based on the idea that personal data protection is a fundamental human right, and it is the same model followed by the CCPA, GDPR, and Jordanian PDPL (Regulation (EU) 2016/679 [GDPR], 2016, Recital 2,4., Khurum et al., 2023). This model implies that personal data should be protected by empowering data subjects to exercise rights over it, such as the right to control the usage of their data by enforcing data controllers to acquire consent before processing it, and the right to privacy over their data by ensuring its confidentiality and security (Shehu and Shehu, 2023).

This approach focuses on protecting personal data by prohibiting unlawful processing. However, PDPLs regulatory systems include many exceptions that allow data controllers to process personal data without individuals' prior consent. Hence, it is safe to argue that this approach focuses on personal data protection as a fundamental right, but not the full right of privacy (Deterrmann, 2019).

Art. (21/C) of the Jordanian PDPL of 2023 and Arts. (79) and (82) of the GDPR explicitly state that everyone who suffers any material or non-material harm has the right to pursue a judicial remedy and to receive compensation from the controller or processor. This indicates that, on human rights grounds, while individuals can benefit from data protection authorities to enforce some of their rights, this approach relies on tort law as the legal regime for protecting personal data. However, protecting personal data by using this mechanism may create some challenges for individuals, some authors argue (Bergelson, 2003 and Purtova, 2010) that tort law is insufficient to provide the proper protection over personal data, as this regime lacks proactive mechanisms, and it is dependent on whether the individual was harmed because of that violation of his privacy or not, not to mention that the concept of damage varies from one society or individual to another according to different circumstances. Case law provided another limitation with the tort law approach is that the illegitimate action that constitutes the violation of privacy may vary from case to case, for example, courts in the UK used the concept of breaching confidentiality, while in Canada, they have relied on intrusion upon seclusion (Jones v Tseige [2012] as cited in: Trakman et al., 2019). In a new verdict, the court of appeal in England and Wales considered that the unlawful processing and the "fear of misuse" as a non-material harm are sufficient to create a legal ground for compensation, and thus, the threshold for seriousness does not apply under GDPR and the Data Protection Act of 2018 (Farley v Paymaster, 2025). Still, what would be considered a privacy violation in one society might not be considered a violation in another, even though they are in the same country and subject to the same legal system, not to mention the exceptions that sometimes.

5.2. informational self-determination:

First introduced by the German Federal Constitutional Court in the famous census case of 1983, this model implies that information self-determination emanates from the right to personality, a fundamental human right, and serves as a legal basis for the right to personal data protection. Therefore, the right of self-determination shall not be restricted except only if there is an overriding public interest (Bundesverfassungsgericht, 15. Dec, 1983).

This approach relies on two mechanisms: an inactive one, when the controller informs the data subject with processing details, and an active mechanism, which appears when the data subject has the authority to influence the flow of processing activities (Vivarelli, 2020). Informational self-determination is based on an analogy between the "self" and "personal

information”; therefore, whoever exercises control over his personal data exercises control over himself. Hence, this right gives individuals the freedom to choose and determine how information should be disclosed and used. This understanding was taken by some legislators in Europe, including the French legislator (Thouvenin, 2021).

Given the common legal ground of this and the human rights approach, which is the fundamental rights ground, some authors argue that this model serves as the rationale for the GDPR and other PDPL models. However, if this were the case, data subjects should have been granted more authority and control over their data than they already have, especially against the private sector, and consent should be the central legal ground for lawful processing (Thouvenin, 2021).

While informational self-determination tends to be stricter than the human rights approach regarding personal data control, there are still some unaddressed issues regarding this model's ability to serve as a tool for protecting personal data. First, like the human rights model, this approach enables data subjects to control the personal data they voluntarily provide to data controllers, but tends to be less efficient for inferred data, or the data that controllers acquire from 3rd parties. Furthermore, informational self-determination entails many challenges related to data asymmetry, as well as doubts about the effectiveness of the consent mechanism and the privacy paradox (Verhulst, 2023; Vivarelli, 2020).

5.3. Risk-Harm Assessment Model:

From daily practice in governance and compliance of data protection laws to a separate data protection model, the risk or harm-based model is one that is based on the idea of organizational governance (Centre Information Policy Leadership, 2014). Despite the claims that this approach is not aiming to replace the current personal data protection legal systems, it serves as an approach for personal data protection that aims to avoid the impediments of the other approaches (Bambauer, 2024). The approach aims to strike a balance between the need for a flexible personal data ecosystem and the preservation of individuals' privacy. Hence, this approach implies a criterion categorization for personal data practices into three categories: a violation, a non-violation, and the in-between classification (Bambauer, 2024). While the first two classifications are, to some extent, objective and clear and may not be a major problem, the last one is somewhat subjective and vague.

Legitimate processing may be grounded in clear and objective bases, such as consent, public interest, the best interests of the data subject, and others (Bambauer, 2024). Nevertheless, the last category raises some contentions. Given the dynamic nature of the personal data ecosystem and the continuous development of technology, it is difficult to determine which processing is appropriate and which is inappropriate, and leaving the decision to entities would lead to inconsistent results. Furthermore, this model is based on the idea of a risk assessment conducted by data controllers, although it may also be based on rigorous organizational standards. The case may differ from one sector to another, and from one controller to another. Finally, this model does not provide a clear enforcement system for data subject rights, for instance, to what extent can the data subject exercise his right to object to the process if the risk is low? And how could the data subject know the risk to his data?

5.4. The data fiduciary model:

This model supposes an imbalance of power between the parties in the relationship, when the weaker party is outweighed by the stronger one and cannot practice equal authority to what the stronger one can practice against them. In other words, this model implies that it is an acquiescence relationship (Balkin, 2020). Given the nature of such a relationship, this approach relies on the concept of “trust-ship,” in which businesses act as trustees for the beneficiary's benefit. In other words, the trustee is obliged to act in good faith and in the beneficiary's best interests (Dobkin, 2017).

In the context of personal data, this approach implies that data subjects and individuals provide their data to entities by virtue of trust, and data fiduciaries have some obligations in favour of data subjects, for instance, the duty of care and confidentiality, as well as loyalty (Balkin, 2020). Taking into account that the relationship between data subjects and data's fiduciaries is based on trust, fiduciaries need to be as transparent as possible in order to gain the trust of individuals, as surveys show that transparency encourages individuals to provide their data (Oulasvirta et al., 2014); in other words, transparency creates trust.

This approach implies that fiduciary duties should not only apply to data fiduciaries but also to third parties, such as data

brokers and data collectors, who do not have a legal relationship with end users or data subjects. Ergo, the individuals should have the same authorities that they have against fiduciaries against third parties (Balkin, 2020).

A fiduciary relationship between the data subject and the data controllers may be suitable for addressing many issues related to personal data privacy. However, this idea faces some legal and practical challenges. First, this idea is well-suited to protecting personal data voluntarily provided by individuals, in line with the idea of trust-ship. As previously discussed, personal data can be collected through various approaches, including volunteer data. Thus, a question may arise about the margin for applying this idea to data collected involuntarily, such as inferred data, and to data bought from 3rd parties, such as data brokers and other data merchants, or the data that is acquired through the internet by algorithmic systems (Khan & Pozen, 2019). Furthermore, this approach is based on analogies between the relationships between individuals and controllers, and between individuals and professionals, such as doctors and lawyers.

While this is a plausible approach, it still has some difficulties. For instance, the doctor shall work in his patient's best interest, and the criteria here are, to some extent, clear, providing healthcare and treatment to his patients. The same goes for the lawyer; however, regarding the ties between the data subject and the controller, behavioral advertising may be an unresolved issue. In the context of social media, even authors who promote this model admit that behavioral advertising is not uniform (Balkin, 2020); some ads may be considered in favor of data subjects, while others may not. However, there is no clear, unified interpretation of the “best interest” criterion; its interpretation varies depending on factors such as the type of application and the type of data processed, as well as whether it will be shared with 3rd parties (Tang et al., 2025). Another issue with this model is the ambiguity of the preemptive mechanism. While this approach stands on tort, restitution, punitive damages, and injunctions as a compensatory basis to address consequent harm (Filler et al, 2022) Preemptive measures, data subject rights, and finally, given the contradicting relationship between fiduciary obligations against stockholders and their duty of loyalty, a conflict of interests arises (Khan & Pozen, 2019).

Based on the foundation above, it appears that, on one hand, each model suffers from its own gaps, and on the other hand, the four addressed models face a challenge in terms of inferred data, the data that have not been collected from individuals directly and upon his consent or choice. On the other hand, the ownership model proposed in this paper is likely to overcome these obstacles. Yet it is necessary to examine the current PDPL status quo regarding the idea of personal data ownership before examining it.

6. The position of PDPLs regarding property rights.

As previously noted, PDPLs were enacted to protect personal data and to strike a balance between fundamental rights and economic progress. However, protecting fundamental rights to privacy may not be achieved by attributing ownership of personal data to individuals. Nevertheless, it is necessary first to examine the rules of PDPLs, as they are the legislative systems that regulate personal data and its protection.

6.1. Linguistic analysis of personal data statutory definition:

It is essential, before diving deeply into the legal analysis of PDPL's provisions, to provide a linguistic analysis of the definition of personal data. Personal data is defined in the GDPR as “any information that relating to an identified or identifiable natural person,” (Regulation (EU) 2016/679 [GDPR], 2016) and in the Jordanian PDPL as “Any data or information related to a natural person that directly or indirectly identifies them...” (Jordanian personal data protection law, 2023) while in California privacy consumer Act as “means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household” (California privacy consumer Act, 2018).

The first note about the common factor between the previous definitions is that they do not provide any explicit linguistic expression of ownership over personal data; both the GDPR and Jordanian law take a similar approach to identifying personal data, stating that it is “any information related to”. A similar approach is taken by CCPA as it uses the terms (that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked).

Therefore, we need to examine the semantic aspects of the terms used. According to recital 26 of GDPR, “the principles

of data protection should apply to any information concerning an identified or identifiable natural person.” The recital interprets the term “related” as “concerning,” i.e., data that concerns an identified or identifiable individual. From a semantic perspective, the phrase “related” carries multiple meanings. According to the Cambridge dictionary, “related” means “connected to”, “influenced by”, and “Caused by something” (Cambridge, n.d.).

When information is related to a specific individual, it is about him or her and reveals something about the identified or identifiable person (Finck and Pallas, 2020). From a semantic perspective, the word “related” does not primarily mean “owned”; rather, it indicates the connection or relationship between the individual and the data, rather than the individual's entitlement to property over their data. Similarly goes to the terms used in CCPA: “identify, related to, describes, associated with, linked to”. In the same vein, the three statutory models share a similar name-culture with individuals, namely “data subject or consumer”; thus, if something is related to someone, that does not necessarily, from a semantic perspective, mean that the latter is the owner of it.

6.2. PDPLS perspective analysis:

Since the linguistic perspective does not resolve the issue of personal data ownership, we must examine the full context of PDPLs to identify any explicit signs of personal data ownership. However, we may be compelled to examine the data subject rights provisions stipulated in the PDPLS to identify any embedded indicators that can inform this discourse. Nevertheless, such an approach must be taken with respect to ownership rights.

By examining the PDPLs considered in this study, we observe that neither the Jordanian PDPL, the GDPR, nor the CCPA includes any explicit reference to data ownership. In fact, some authors under the scope of GDPR provisions, attribute the property of data to the controller rather than the individual (privacyengine.com, 2023); however, this claim is nothing but merely an opinion, considering that the GDPR defined the controller as “‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...” so the focal point of identifying the controller is the authority to determine the purposes and means of processing the personal data (Fashion ID, 2019; Jehovan todistajat, 2018; Nacionalinis visuomenės sveikatos centras, 2023; Wirtschaftsakademie Schleswig Holstein, 2018)

Given the foundation above, we need to search deeply for any embedded signs. In this context, PDPL regulations state that the data subject (the consumer) has the authority to exercise various rights, including restricting processing, updating or correcting personal data, and erasure or deletion of processed personal data.

Notwithstanding this, the question is whether the authorization of individuals to exercise multiple rights relevant to their data should be taken to imply that they own their data? If we made a brief comparison between the rights that PDPL grants to Data subjects and property rights granted to “owners” by the Civil Code, we would find a tremendous difference between the two rights “packages”. Therefore, the purpose of this analysis is to determine whether we are the owners of our data under PDPLs, within the bundle of ownership or property rights defined by civil codes.

6.2.1. The right to use and to dispose of the property:

According to both the Jordanian and French civil codes, the owner shall have the right to sell, lease, and exercise any legitimate act with respect to his property (Jordanian Civil Law, 1976). On the other hand, we notice that PDPLs have allowed other parties to process, dispose of, and use personal data in many cases without the consent or permission of data subject, but on different levels with respect to the scope of usufruct (Jordanian Personal Data Protection Law of 2023, and Regulation (EU) 2016/679 [GDPR], 2018).

6.2.2. The right to exclude others from using the property:

The owner not only uses, usufructs, and disposes of his property, but also has the right to exclude others from enjoying such rights over it (Jordanian civil law of 1976). In the vein of PDPLs, the authority to exclude others from using your data may be interpreted as falling within the concept of withdrawing consent and the right to have personal data erased. Notable that property rights upon personal data should be reflected mainly by the right to exclude other parties from personal data usage (Purtova, 2015).

Based on this foundation, we can infer that Jordanian PDPL allows the data subject to exercise the rights set out in Article

4, including the right to withdraw consent, the right to erasure, and stop processing. However, the data subject can not deprive the controller from using or processing his data except if the process itself was based on prior consent or if the process itself was illegal. In addition, he can not require the controller to erase his data unless the processing was conducted with prior consent or is illegal. (Jordanian personal data protection law, 2023). In “contrario”, if the process was performed under an exception to obtaining the Data subject’s consent, they cannot deprive the controller of using it, which means the personal data can not be erased by their own will (Jordanian personal data protection law of 2023).

GDPR also adopted a parallel position regarding this issue. According to Article 17, the right to erasure (to be forgotten) can not be practiced except in a limited number of cases, such as withdrawing consent if the process was based on it or if it was unlawful or for compliance with a legal obligation, etc. (Regulation (EU) 2016/679 [GDPR], 2018). The California Consumer Privacy Act of 2018 provides a clearer approach to the right to delete personal data. According to section (1798.105), the consumer has the right to request that the business erase their personal information. The business in this case shall comply with that request. In addition, if the personal information is in the hands of a third party, such as a contractor or business provider, that party shall collaborate to fulfill the consumer's request. However, this right is not absolute; some exceptions may permit the business to retain the data (California Consumer Privacy Act of 2018). Overall, allowing individuals some degree of control over their data does not necessarily mean that they own it (Graux, 2024). Thus, this study disagrees with the scholarship that says that GDPR and CCPA adopt the legal framework of property over personal data (Bambauer, 2024.).

7. Alternative Legal basis for data ownership:

The previous approach indicates that PDP regulatory systems, the subject of this study, do not grant data subjects ownership rights over their personal data, as they are primarily based on the human rights control model. Nevertheless, that does not mean that data subjects (individuals) do not, unequivocally, own their data. Given that these regulatory systems were issued to regulate personal data protection as a fundamental human right and to balance the privacy of natural persons with social progress (Regulation (EU) 2016/679 [GDPR], 2016, Recital 1, 2, 4). Ergo, an alternative approach should be adopted to identify a legal basis for attributing ownership of personal data to individuals.

It is hardly surprising that personal data is not separated from or unaffected by technological development (Purtova, 2011). However, it is not a new phenomenon, and its existence was not always associated with technological development, even though when it is mentioned, we basically and instantly think of its digital form, like Clickstream, IP addresses, and others. While the fact is that personal data is an old concept that dates back to the beginning of humanity.

The Jordanian Civil Code No. 43 of 1976 provides a straightforward regulatory approach to the inviolability of rights inherent in human nature, which are phrased as civil rights in accordance with the French Civil Code (French Civil Law of 1804). This concept encompasses the name, surname, privacy, safety, reputation, dignity, and other civil rights (Bu Juma’a, 2018). The Jordanian Civil Code emphasizes that a person has the right not only to stop any infringement of their inherent rights, but also to seek compensation if it was justified (Jordanian Civil Law, 1976).

The concept of inherent rights includes the right to a name, the inviolability of one's image, voice, and other sensitive information (Bu Juma’a, 2018). If we address the definition of inherent rights, as set out by the Civil Code literally, then, a certain personal data may be considered as an extension of the inherent or civil rights that legally and logically belong to individuals, and no party shall have the authority to dispose of it unless under the provisions of the Law and within the limits of public interests.

The foundation above lays the groundwork for the idea that individuals have some authority and the ability to exclude third parties from using their personal data. However, it is not sufficient and clear enough to provide a solid legal basis for ownership rights. Taking into consideration that inherent rights are inalienable, which is a legal fact that contradicts the status quo of the personal data market worldwide, where personal data is considered one of the most valuable assets (Hazel, 2020). Moreover, classifying personal data as an extension of inherent rights does not unmistakably mean that all categories of personal data are considered part of inherent human rights, for example, a name, title, voice or image are classified as

personal data and inherent rights at the same time, based on the approach above, it does not mean that all personal data are falling into this category. Personal data includes browsing data correspondences purchases, and other types of dynamic data (Parkinson, 2018). While the name and title of voice could be considered an extension of inherent rights, dynamic data such as browsing, financial, and other types are not clearly addressed by this definition.

In a related development, given the legislative gap, ownership is also a natural right. Natural rights (Human rights) are general and moral rights and are obtained from the General morals (Finnis, 2011). That means it does not need to be stipulated by the legislature to exist or be admitted. Property rights are, therefore, needless to be agreed upon socially (LON L. FULLER, 1966 as cited in Sandefur, 2023). Ownership of personal data may still be an authentic right, because many forms of personal data are part of the person themselves, such as Biometric data. While others are derived from the people themselves or inferred from their behavior or orientations. Thus, according to natural law principles and analogy, personal data is a part of self-ownership. Self-ownership is being granted to people as per their humanity (Sandefur, 2023). This approach contradicts the idea that ownership is a right that needs to be posited by a superior authority or agreed upon socially or is a perquisite awarded to the individual by social agreement, which means that we own our data by default (*de facto*), not by legal order (*de jure*) (Janeček, 2018). If there were a place for analogy in this case, we could measure ownership of personal data in terms of our bodies and limbs, or our intellectual outputs.

8. Discussion

As established in previous chapters, the ownership of personal data is an intractable jurisprudential debate. However, this right is necessary to protect our data and privacy. While the contemporary Human rights model PDPL regulatory framework provided a paradox, aiming to protect personal data on one hand and achieve economic progress on the other hand, it does not provide a legal ground for personal data property, hence it does not equip individuals with the necessary proprietary tools and mechanisms to face the consequences of the digital data-driven economy ecosystem. Simultaneously, one must not overlook the fundamental premise that ownership or property rights are an inherent and natural human right, meaning that there is still a place to propertize personal data based on the existing rules of the Civil Code, taking into consideration the flexibility of the concept of objects of property and their dynamic and evolving nature (Purtova, 2010).

This paper proposes integrating personal data into the property concept in a manner that guarantees the individual's control over their data and aligns with the digital economy ecosystem and the current personal data market and, at the same time, fill the gaps and issues that the formerly examined control models could not. As previously discussed, property includes both tangible and intangible assets. Thus, there is no legal issue with identifying an intangible asset as property, as with intellectual property, given its non-rivalrous nature, which the concept of intellectual property accommodates.

The proposed model is a conceptual framework for personal data ownership, similar to the intellectual property framework (Savona, 2019 and Bergelson, 2003), in which the data subject has a moral right (attribution) and an economic one (utilization). Based on this foundation, personal data ownership will encompass two aspects: the personal, or “in personam,” and the real, or “in rem,” aspect. The in personam and in rem model is a unique, but not new, approach derived from Roman law, based on the distinction between in personam and in rem rights of property. This approach has evolved differently in both civil and common law systems (Blicharz, 2024).

Based on the foregoing, an individual is the owner of his personal data. Hence, he is the “in-rem right-holder”. To apply this model, an individual can transfer some of his authorities to the controller and can grant the controller a lease of his data or a usufruct right. The individual therefore retains his authority as an owner, while the controller or third parties operate within the scope of the authorities transferred to him, which may consider the legitimate interest of the controller to process the data for the purposes for which it was collected for (Bergelson, 2003).

A result of applying such a paradigm will be that controllers or aggregators not only cannot dispose of personal data to third parties without the consent of the in-personam right-holder, but that the latter (as an in personam right holder) also has the right to acquire a recompense for the transfer of their in-rem right to them (Rees, 2014). Moreover, This approach may equip individuals with more efficient control over their data and may help them in stopping the violation of their personal

data on the other hand (Janeček, 2018) On the other hand, it would help organize the market, as businesses and data aggregators will be forced to compensate individuals whose data is processed. Indeed, applying such a model will require comprehensive reforms on both practical and legislative fronts. However, this model seems to align with the way the personal data ecosystem operates.

The ownership model, unlike other control models, will equip data subjects with the authority to protect their personal data, whether it was provided voluntarily, inferred, or acquired from third parties, taking into account the “Erga omnes” effect of ownership (Purtova, 2010). That said, ownership should not be taken as an absolute exclusive right, and some sort of balance needs to be struck between personal data market shareholders.

9. Conclusion

Property rights over personal data are a long-standing, controversial debate, as the two rights have long been interrelated; many arguments push for and against it. Yet, personal data ownership appears to be a crucial safeguard of the right to privacy. Property rights have both positive and passive aspects and are defined primarily by the right to exclude others from using your property. In the same development, the Jordanian civil code adopts a broad, flexible model of property that encompasses both tangible and intangible property, provided it can be possessed and is not excluded from dealing by the rule of law.

By examining the major control models in this area, mainly, human rights, fiduciary, risk-based, and self-regulatory determination, it appears that each model has its own positives; however, each model has its own gaps and deficiencies as well. Moreover, there is a common challenge for them: handling inferred and observed personal data. On the other hand, the ownership model seems to overcome this challenge and provide a clearer approach towards protecting personal data. However, given that these laws are based on the human rights model, the examined PDPL regulatory systems do not include a clear approach to identifying who owns personal data.

The Jordanian and French civil codes provide safeguards regarding inherent or civil rights, a concept that encompasses certain types of personal data, such as name, image, voice, and private life. Civil Codes equipped individuals with some authority to prevent and punish any violation of their inherent rights. However, it is not sufficient and clear enough to provide a solid legal basis for ownership rights. Taking into consideration that inherent rights are inalienable, which is a legal fact that contradicts the status quo of the personal data market worldwide.

While admitting the legislative gap, we should never forget that ownership is also a natural right. That means it does not need to be stipulated by the legislature to exist or be admitted. Ownership of personal data may still be an authentic right, because personal data is whether a part of or emitted by the person themselves, such as Biometric data. While others are derived from the people themselves or inferred from their behavior or orientation, etc.

This paper suggests integrating personal data into the concept of property in a manner that guarantees the individual's control over their data and aligns with the digital economy ecosystem and the current personal data market. To achieve this purpose, the study provides a new model for personal data ownership, similar to the model of intellectual property, in which individuals retain their moral ownership rights over their data while disposing of the economic side of their ownership through in rem and in personam approaches. This approach may equip individuals with more efficient control over their data, help them stop unauthorized use of their personal data, address issues related to inferred data, and help organize the market.

References

- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442–492. <https://doi.org/10.1257/jel.54.2.442>
- Al-Khoury, A. (2012). Data ownership: Who owns “my data”? *International Journal of Management & Information Technology*, 2(1), 1–8.

- Balkin, J. (2020, January 10). The fiduciary model of privacy. *Harvard Law Review Forum*.
- Bambauer, J. (2024, April 22). How to get the property out of privacy law. *The Yale Law Journal Forum*.
- Bell, A., & Parchomovsky, G. (2019). The privacy interest in property. *University of Pennsylvania Law Review*, 167, 869–920.
- Bergelson, V. (2003). It's personal but is it mine? Toward property rights in personal information. *University of California Davis Law Review*, 37, 379–451.
- Blicharz, G. (2024). Law and the study of the commons: The in personam and in rem rights paradigms. In P. Hellwege & M. Soniewicka (Eds.), *Law and interdisciplinary* (pp. 283–316). Mohr Siebeck.
- Bu Juma'a, Y. (2018). الحقوق الملازمة للشخصية وتقسيماتها: دراسة مقارنة على ضوء القانون والفقه والقضاء [Inherent rights and its categories: A comparative study based on law, jurisprudence, and judiciary]. *Legal Studies Journal – Sovereignty and Globalization Section*, 4(1), 341–359.
- California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 (2018).
- Code Civil* [Civil Code] (1804) (G. Rouhette, Trans.).
- Court of Justice of the European Union. (2024). *Fact sheet: Protection of personal data*. <https://curia.europa.eu>
- D'Hauwers, R., & Vandercruysse, L. (2025). Competitive advantage and personal data ecosystems: A typology of personal data control constellations. *Journal of Theoretical and Applied Electronic Commerce Research*, 20(1), 1–23. <https://doi.org/10.3390/jtaer20010008>
- Determann, L. (2019). Privacy and data protection. *Moscow Journal of International Law*, (1), 18–26. <https://doi.org/10.24833/0869-0049-2019-1-18-26>
- di Robilant, A. (2012). Common ownership and equality of autonomy. *McGill Law Journal*, 58(2), 265–320. <https://doi.org/10.7202/1017516ar>
- Dobkin, A. (2017). Information fiduciaries in practice: Data privacy and user expectations. *Berkeley Technology Law Journal*, 33(1), 3–50.
- Esmaili, H., & Grigg, B. (2016). *The boundaries of Australian property law*. Cambridge University Press.
- Filler, D., Haendler, D., & Fischer, J. (2022). Negligence at the breach: Information fiduciaries and the duty to care for data. *Connecticut Law Review*, 54(1), 105–149.
- Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11–36. <https://doi.org/10.1093/idpl/ipz026>
- Finnis, J. (2011). *Natural law and natural rights*. Oxford University Press.
- Graux, H. (2024). *What is data ownership, and does it still matter under EU data law? An exploration of traditional concepts of data ownership, and of the expected impact of the Data Act*. Data.europa.eu.
- Hazel, S. (2020). Personal data as property. *Syracuse Law Review*, 70, 1055–1112.
- Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer Law & Security Review*, 34(5), 1040–1052.
- Jordanian Civil Law No. 43 of 1976, Official Gazette No. 2645.
- Jordanian Law of Author Rights No. 22 of 1992, as amended.
- Judgment of December 15, 1983, *Bundesverfassungsgericht* [BVerfG] [Federal Constitutional Court], 65 BVerfGE 1.
- Katz, L. (2017). Philosophy of property law, three ways. In J. Tasioulas (Ed.), *The Cambridge companion to the philosophy of law* (pp. 371–389). Cambridge University Press.
- Khan, L., & Pozen, D. (2019). A skeptical view of information fiduciaries. *Harvard Law Review*, 133, 497–540. <https://ssrn.com/abstract=3341661>
- Khurram, S., Naqvi, H., & Batool, K. (2023). A comparative analysis between General Data Protection Regulations and California Consumer Privacy Act. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, 4(1), 326–332.
- Litman, J. (2000). Information privacy/information property. *Stanford Law Review*, 52(5), 1283–1313. <https://doi.org/10.2139/ssrn.218274>
- Michele, F., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the

- GDPR. *International Data Privacy Law*, 10(1), 11–36. <https://doi.org/10.1093/idpl/ipz026>
- Mingaleva, Z., & Mirskikh, I. (2015). Psychological aspects of intellectual property protection. *Procedia – Social and Behavioral Sciences*, 190, 221–226.
- Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior, and Social Networking*, 17(10), 1–6. <https://doi.org/10.1089/cyber.2013.0585>
- Parkinson, B. (2018). *Personal data: Definition and access* (Doctoral thesis, University of Southampton).
- Personal Data Protection Law No. 24 of 2023, Official Gazette No. 5881, 4338 (Jordan).
- Pierre, B. (1997). Classification of property and conceptions of ownership in civil and common law. *Revue générale de droit*, 28(2), 235–274. <https://doi.org/10.7202/1035639ar>
- Purtova, N. (2010, September). *Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence* (Working Paper No. 2010/017, Version 1.0). TILT Law & Technology. <https://doi.org/10.2139/ssrn.1641027>
- Purtova, N. (2011). *Property rights in personal data: A European perspective* (Doctoral thesis, Tilburg University).
- Purtova, N. (2015). The illusion of personal data as no one's property. *Law, Innovation and Technology*, 7(1), 83–111. <https://doi.org/10.1080/17579961.2015.1052646>
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- Related. (n.d.). In *Cambridge Dictionary*. Retrieved May 15, 2026, from <https://dictionary.cambridge.org/dictionary/english/related>
- Sandefur, T. (2023). The natural right of property. *Texas A&M Journal of Property Law*, 9(4), 673–706. <https://doi.org/10.37419/JPL.V9.I4.10>
- Savona, M. (2019). *The value of data: Towards a framework to redistribute it*. Science Policy Research Unit. <https://ssrn.com/abstract=3476668>
- Seipp, D. (1981). The right to privacy in nineteenth century America. *Harvard Law Review*, 94, 1892–1910. https://scholarship.law.bu.edu/faculty_scholarship/1568
- Shehu, V., & Shehu, V. (2023). Human rights in the technology era – Protection of data rights. *European Journal of Economics, Law and Social Sciences*, 7(2), 1–10.
- Solove, D. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review*, 53, 1393–1462. <https://doi.org/10.2139/ssrn.248300>
- The official portal for European data. (2024). *What is data ownership, and does it still matter under EU data law? An exploration of traditional concepts of data ownership, and of the expected impact of the Data Act*. <https://data.europa.eu>
- The Supreme Court of the United Kingdom. (2025). *Farley v Paymaster*, Case No. CA-2024-000578.
- Thouvenin, F. (2021). Informational self-determination: A convincing rationale for data protection law? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 246–256. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jipitec12&section=41
- Thouvenin, F., & Tamò-Larrieux, A. (2021). Data ownership and data access rights: Meaningful tools for promoting the European digital single market? In M. Burri (Ed.), *Big data and global trade law* (pp. 317–339). Cambridge University Press. <https://doi.org/10.1017/9781108919234.020>
- Trakman, L., Walters, R., & Zeller, B. (2019). Tort and data protection law: Are there any lessons to be learnt? *European Data Protection Law Review*, 5(4), 1–20. <https://doi.org/10.21552/edpl/2019/4/8>
- Understanding data ownership under GDPR: What you need to know. (n.d.). *Privacy Engine*. <https://privacyengine.io>
- Verhulst, S. (2023). Operationalizing digital self-determination. *Data & Policy*, 5, 1–15. <https://doi.org/10.1017/dap.2023.11>
- Vivarelli, A. (2020). The crisis of the right to informational self-determination. *The Italian Law Journal*, 6(1), 302–316.

- Weir, M. (2015). Pushing the envelope of proprietary interests: The nadir of the *numerus clausus* principle? *Melbourne University Law Review*, 39, 651–679. http://law.unimelb.edu.au/_data/assets/pdf_file/0008/1774556/08-Weir.pdf
- Wendehorst, C. (2022). Of elephants in the room and paper tigers: How to reconcile data protection and the data economy. In C. Lohsse, R. Schulze, & D. Staudenmayer (Eds.), *Trading data in the digital economy: Legal concepts and tools* (pp. 327–355).
- Zambon, A. (2019). Property: A conceptual analysis. *Journal for Constitutional Theory and Philosophy of Law*, 38, 55–73. <https://doi.org/10.4000/revus.5208>
- Zimmerman, D. (1983). Requiem for a heavyweight: A farewell to Warren and Brandeis’s privacy tort. *Cornell Law Review*, 68(3), 292–367. <https://scholarship.law.cornell.edu/clr/vol68/iss3/1>