Ius Humani

Revista de Derecho. Vol. 14 (I) (2025), pp. 137-158. ISSN: 1390-440X — eISSN: 1390-7794

Recepción: 15-04-2025. Aceptación: 22-06-2025. Publicación electrónica: 06-07-2025

https://doi.org/10.31207/ih.v14i1.409

HUMAN RIGHTS AND CONTROL OF PERSONAL DATA IN THE DIGITAL ECONOMY: EU LEGAL CASE STUDIES AND RECOMMENDATIONS FOR VIETNAM

DERECHOS HUMANOS Y CONTROL DE DATOS PERSONALES EN LA ECONOMÍA DIGITAL: CASOS PRÁCTICOS Y RECOMENDACIONES DE LA UE PARA VIETNAM

Vo Trung Hau[*]

Abstract: Personal data is strictly managed and protected because it is a matter related to human rights. According to the European Union (EU) law, personal data control is a fundamental right recognized in the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights. Based on the analysis of the content of EU regulations on this issue, the article recommends improving Vietnamese law. The article recommends that Vietnamese law develops regulations on personal data protection in technology-neutral language. In addition, there should also be specific regulations explaining the term *personal data*. Accordingly, personal data includes not only information that can be linked or associated with a particular individual at the time the data are processed, but also all information that may be linked or associated with that individual during future processing, possibly by technological means that were not yet developed at the time the personal data were collected or generated.

Keywords: Personal data, Control of personal data, Human rights.

[*] Ph.D., Binh Duong University, Vietnam. ORCID ID: https://orcid.org/0009-0006-3560-4359. hauvt@tdmu.edu.vn.

Resumen: *Los datos personales se gestionan y protegen estrictamente por tratarse de un asunto relacionado con los derechos humanos. Según la legislación de la Unión Europea (UE), el control de los datos personales es un derecho fundamental reconocido en el Convenio Europeo de Derechos Humanos (CEDH) y la Carta de los Derechos Fundamentales de la UE. A partir del análisis del contenido de la normativa de la UE sobre este tema, el artículo recomienda mejorar la legislación vietnamita. El artículo recomienda que la legislación vietnamita desarrolle normas sobre protección de datos personales con un lenguaje tecnológicamente neutro. Además, debería haber normas específicas que expliquen el término datos personales. Esto se debe a que los datos personales incluyen no solo la información que puede vincularse o asociarse con una persona en particular en el momento del tratamiento de los datos, sino también toda la información que puede vincularse o asociarse con esa persona durante el tratamiento futuro, posiblemente mediante medios tecnológicos que aún no se habían desarrollado en el momento en que se recopilaron o generaron los datos personales.*

Palabras clave: *Datos personales,* C*ontrol de datos personales,* D*erechos humanos.*

I. INTRODUCTION

Digital economy is a general term for businesses that engage in data-driven activities as part of their core business. This focuses on the secondary use of data, that is, business models that seek to use existing data in different ways to generate profits. In that sense, digital economy refers to business

models that use data as a resource, whether structured or unstructured, manually processed or computerized, personal or non-personal data, etc.

Personal data is strictly regulated and protected because of its human rights implications (European Commission, 2016). However, the EU's primary concern is economic integration, and the first legal regulations were drafted to unleash the potential of the European single market (Middelaar, 2013). Furthermore, the free movement of capital, goods, and services within the European single market requires the free flow of data. Therefore, reaching a standard agreement on unified data protection in the EU becomes extremely urgent.

In the context of digital economy, control is required at three stages in the data value chain: data collection, data analysis, and decision-making (Westin, 2015). The concept of control over personal data is closely related to several important values, such as self-determination, freedom, autonomy, and privacy. These values are the basis for fundamental rights and principles enshrined in EU law. The right to data protection and the right to control data are enshrined in the German Constitution and the ECHR (Stilman, 2015).

II. CONTROL OF PERSONAL DATA IN THE DIGITAL ECONOMY UNDER THE EU CHARTER

II.1. Control of Personal Data Under Article 8 of the ECHR

Human rights are generally defined by their inviolability, universality, indivisibility, interdependence, and interrelatedness (Quane, 2012). Beitz (2009) describes them as "constitutive norms of all activities whose purpose is

to protect individuals from threats to their most important interests […]" (p. 197). Privacy, as a basic human need, applies to many areas of life; however, there is no universally accepted definition (Westin, 2015).

In the late 19th century, Warren and Brandeis introduced the concept of privacy as the right to be left alone. Later discussions have identified various principles related to privacy (Solove, 2002). Since the early 20th century, the understanding of privacy has evolved alongside technological developments. From an information technology perspective, a key concern has been the control of personal data. Westin (2015) emphasized the informational dimension of privacy, stating: "Privacy is the right of individuals, groups or organizations to decide for themselves when, how and to what extent information about them is communicated" (p. 1). Today, many activities across both private and public sectors involve the collection and processing of personal information. As a result, informational privacy is now viewed not as a separate form but as an overarching concept encompassing all aspects of privacy (Koops, 2016).

Moreover, article 12 of the Universal Declaration of Human Rights affirms the right to privacy, protecting individuals from arbitrary interference with their family, home, or correspondence (Hustinx, 2015). Similarly, article 8 of the ECHR protects "private and family life" and "home and "correspondence". The European Court of Human Rights (ECtHR) has interpreted this provision in various ways, recognizing privacy as secrecy or seclusion, non-interference and liberty (De Hert and Gutwirth, 2006), autonomy, and control over personal data (Hustinx, 2015).

The ECtHR has also held that data protection principles derived from the Council of Europe Convention on automated personal data processing

require that data storage is proportionate to its purpose and limited in duration. Moreover, disclosing personal data to third parties can constitute a violation of the ECHR. The widespread availability of personal, especially sensitive, data can jeopardize protections for both privacy and family life. Even a private press release not intended for online distribution can be intercepted and circulated online, harming the individual's privacy and personal relationships.

The Organization for Economic Co-operation and Development (OECD) defines personal data as any information that relates directly or indirectly to an individual. However, in the Magyar Helsinki Bizottsag case, the Court abandoned this approach and adopted a narrower definition of personal data in the public domain. Judges Nussberger and Keller rejected the argument that data already in the public domain and published requires less protection. Protecting personal data is an important determinant that must be ensured regardless of whether the data is in the public domain or remains confidential.

In this view, the concept of "private life" under article 8 should, in principle, continue to protect both published and unpublished personal data. In defining the boundaries of article 8 about personal data, the two judges also relied on the recent judgment of the European Court of Justice (CJEU) on EU data protection. This dissenting opinion is an important recognition that, in the digital economy, personal data must not only be limited to the private sphere to ensure privacy protection but must also be extended. Even if a person wants to keep the data to himself, this is becoming increasingly difficult. Therefore, the Court must acknowledge the need to protect personal data in the digital economy.

Before the Charter of Fundamental Rights of the EU came into force on December 1, 2009, the CJEU dealt with cases related to privacy and data protection, based mainly on the principles and case law established by the ECtHR (Case C-93/09 Hartmut Eifert v Land Hesse, 2010). This approach reflects the absence of a unified and binding legal framework at the EU level. However, a significant shift has occurred with the Treaty on the Functioning of the European Union (TFEU), which gave the Charter binding legal force. This has allowed the CJEU to directly refer to the Charter's provisions, including article 7 on privacy and, in particular, article 8 on data protection, in its judgments since 2009.

This change marks a shift from applying external standards to establishing a EU system to protect fundamental rights. The TFEU strengthens the Charter's legal standing and affirms data protection as a fundamental right, separate from but closely related to the right to privacy. This makes article 16 of the TFEU a clear legal basis for enacting data protection law at the EU level. Therefore, reaffirming the fundamental nature of the right to data protection and facilitating its enactment are important steps forward. This demonstrates the EU's strong and consistent commitment to protecting personal data in the digital economy (Hijmans, 2016).

However, this development is not only of legal significance but also reflects a change in the perception of the importance of personal data protection in modern society. Personal data protection is not only an individual right but also a key factor in ensuring trust and the development of the digital economy.

II.2. Control of Personal Data Under Article 7 of the EU Charter of Fundamental Rights

Article 7 of the Charter of Fundamental Rights of the EU provides everyone with the right to respect for private and family life, home, and communications. Since the provisions of article 7 of the Charter of Fundamental Rights of the EU are similar to article 8 of the ECHR, the case law of the ECtHR is an important reference (cases C-465/00, C-138/01, C-139/01, 2023). Likewise, the CJEU has interpreted article 7 to include individuals' physical, psychological, and moral aspects of personal integrity, identity, and autonomy (Peers, 2014). In that sense, the right to privacy under article 7 of the Charter of Fundamental Rights of the EU has been used to protect against house searches, ensure the confidentiality of communications, and ensure environmental protection. As for articles 8 of the ECHR and 7 of the Charter of Fundamental Rights of the EU, these also protect the right to personal data.

In the ASNEF (National Association of Financial Credit Institutions) case, the CJEU held that the breach of non-public data constitutes a " serious violation of the rights of the data subject" under articles 7 and 8 of the Charter (Case C-468/10 ASNEF, 2011). Facing this, the Charter introduced a new right to data protection in article 8. This is closely related to article 7, as the protection of personal data and a person's dignity are linked, and this close relationship is why the inclusion of article 8 in the Charter did not significantly change the CJEU's reasoning on the right to privacy. Typically, the Court conflates the two rights (Lynskey, 2015); the question, therefore, arises as to why the new right was implemented in articles 8 and 7, which are almost always interpreted as a

whole. Why does article 7 not provide adequate protection for personal data? The EU Charter defines the right to data protection in article 8. This provision guarantees personal data protection for all persons to whom the data relates:

> The data shall be processed fairly for the specified purposes and based on the consent of the person concerned or some other lawful basis established by law. The Charter also provides "the right of access to the data collected concerning that person and the right to rectify such data".

The digital economy treats personal data as an economic resource. Therefore, control over personal data points to the potential for personal data protection in the digital economy. However, the rationale for drafting this new right in the Charter and the TFEU in delimiting the right to personal data protection is unclear. Recent cases by the CJEU have clarified that EU law does not help address these two rights. The interpretation of the two rights has given rise to many problems that have not been clearly explained. Therefore, making article 8 of the Charter does not mean anything for the control of personal data in the digital economy. To predict what this right might bring to the control of personal data in the future, it is necessary to clarify two issues: (i) what is the rationale for regulating personal data protection as a human right?, and (ii) how does the right to personal data protection differ from the right to privacy? The first consideration of the right to data protection predates the Charter of Fundamental Rights of the EU. In the face of new technological developments in the early 1970s, the Council of Europe concluded that article 8 of the ECHR had some limitations (Bosco, 2015).

This was one of the first moments when the idea of a standalone right to personal data protection was publicly expressed. In the following years, three

important reasons led to the creation of the new right. First, the EU data protection regime needed more legitimacy. In the 1990s, the EU adopted secondary legislation to protect personal data in circulation within the internal market. On the one hand, the objective of the personal data protection regime is to support the free flow of information.

On the other hand, it also includes protecting personal data and privacy. While the objective of free movement is fully compatible with the EU treaties' single market objective, protecting personal data lacks the necessary foundation in the treaties. Without a standard legal basis, EU data protection law would be reduced to a mere set of rules governing the flow of personal data (Lynskey, 2015). Furthermore, controlling personal data must embrace the changes in society brought about by new digital technologies. According to Lawrence Lessig, constitutional amendments are not simply changing legal provisions. The deeper purpose of such amendments is to influence the core elements of the current legal culture, to create a fundamental change in future social life, and to reshape part of the cultural value system (Lessig L, 2006).

According to De Hert and Gutwirth, the EU Charter has undergone a significant transformation, which is reflected in new provisions on data protection and dignity (De Hert and Gutwirth, 2009). The CJEU has addressed many complex legal issues related to data protection in the context of the digital economy. In that sense, the CJEU's judgments have shed light on important issues, such as the way personal data is protected on the internet (Case C-101/01, 2023), the balance between the right to personal data protection and the right to privacy with other fundamental rights (Case C-275/06, 2008), the scope of the right to personal data protection in the context of rapidly developing

technology (Case C-582/14, 2016), and the identification of the subject responsible for ensuring information privacy. By addressing these cases, the CJEU has developed its legal doctrine and demonstrated its explicit acceptance of Lessig's view of constitutional interpretation in the direction of a "techno-constitution".

However, data protection is not limited to the protection of privacy but also plays an important role in ensuring other legal objectives. One objective is the right to informational self-determination, which was mentioned by the ECtHR in a recent dissenting opinion. Similarly, the CJEU has confirmed that data protection can protect legal values distinct from the right to privacy. These legal values go beyond the scope of the right to privacy, which may explain why data protection objectives cannot be solely enshrined in article 7 of the Charter. Moreover, control of personal data and privacy are closely related but not interchangeable.

In many respects, the right to data protection is narrower in scope than the right to privacy; the latter applies when the right to personal data protection does not apply, as in cases of physical privacy infringement or when data is anonymized (Lynskey, 2015). However, the right to personal data protection can also be broader than the right to privacy (Case T-194/04, 2007). This is the case when personal data has been intentionally made public, meaning that the right to privacy has been waived and is, therefore, not protected under article 7 of the Charter. Nevertheless, in these cases, the right to personal data protection still applies (Lynskey, 2015). The Magyar Helsinki Bizottsag case noted that the protection of personal data is closely related to the concept of informational self-determination, which must be guaranteed regardless of whether the data

has been made public or remains confidential. In the United States, publicly disclosed data falls outside the scope of Fourth Amendment privacy protections.

In addition to the difference in scope, personal data control and privacy are distinguished by different underlying objectives. Lynskey identifies two reasons: (i) the development of individual personality, and (ii) the reduction of power and information asymmetries between individuals and those processing their data (Lynskey, 2015). The first objective concerns the decision of the German Federal Constitutional Court on the census law. In this judgment, the Court relied on the right to informational self-determination to resolve the dilemma of collecting and processing personal data on a large scale.

In the Court's view, any processing of personal data must be considered an interference for the right to informational self-determination unless the data subject has given their consent (Hustinx, 2015). In other words, the right to informational self-determination requires that everyone is able to decide for themselves whether their personal information is disclosed or used. The German Court did not apply the right to privacy but relied on the first article of the German Constitution on protecting human dignity.

Therefore, it can be seen that the right to information autonomy is very different from the idea of privacy as "the right to be left alone". The right to information autonomy is related to the active presence of data, so it is more compatible with the right to personal data protection (Hornung & Schnabel, 2009); it is the basis of the right to personal data protection in the digital economy (McDermott, 2017).

In practice, despite arguments about the distinction between privacy and personal data protection, the CJEU conflates the two rights when dealing with cases that arise (Kokott & Sobotta, 2013). Hijmans (2016) argues that considering these two rights as a whole is the solution to the dilemma:

> Due to the characteristics of the Internet and the development of Internet-based communications with big data and mass surveillance, any processing of personal data is likely to hurt the right to privacy under article 7 of the Charter, if only because one cannot know in advance the purpose for which the personal information available in electronic databases will be used. (p. 36)

According to Hijmans, the rights provided for in articles 7 and 8 of the Charter should be considered a unified whole. The provision on personal data protection in article 8 contains a balancing objective that can be overshadowed if considered solely with the objectives of protecting privacy. On the other hand, constructing the right to data protection as an independent legal concept is important in the context of the digital economy for two reasons.

First, it establishes substantial legal obligations for all subjects to consider professional data protection issues. Carefully, this does not mean personal data protection is only guaranteed when specific legal provisions exist. The case law of the CJEU has developed new rights from constitutional principles, so it is possible to develop a new right, the right to personal data protection, from the right to privacy. In addition, article 16 of the TFEU and article 8 of the Charter require attention to protecting personal data.

Second, the legal provisions on personal data protection will establish a legal framework for subjects processing personal data. In addition, the new

legal provisions on rights also emphasize the importance of individuals applying self-protection methods in deciding how their data is used.

II.3. Control of Personal Data as Defined in Article 21 of the EU Charter

Article 20 of the EU Charter states that: “Everyone is equal before the law", and article 21 of the EU Charter states that discrimination is prohibited: "On any ground such as sex, race, color, ethnic or social origin, genetic characteristics, language, religion or belief, political or other opinion, membership of a national minority, property, place of birth, disability, age or sexual orientation". Moreover, the CJEU defines direct discrimination as that occurring when a person is treated less favorably than another on one of the protected grounds (Watson & Ellis, 2012). In contrast, indirect discrimination occurs when some practice is adopted, or another action is taken that negatively impacts a protected group of people (Watsony Ellis, 2012).

The requirement or practice itself may not be prohibited, but the consequence of the conduct is a distinction between people on the prohibited grounds. In limited circumstances, the Court has permitted discrimination. However, such unequal treatment must be based on objective considerations, independently of the persons’ concerned's nationality, and proportionate to the legitimate objective pursued. In addition, positive discrimination may be lawful when it benefits groups in society that are traditionally mistreated because of their race, gender, or sexual orientation.

In that order of ideas, using personal data in the digital economy increases the risk of discrimination, especially indirect discrimination. Personal data and data reuse can be beneficial for profiling purposes, but the results of

profiling and other types of data analysis can be stigmatizing or discriminatory. Algorithms that leverage personal data analysis can find correlations between risk and disadvantaged groups based on non-causal factors without using personal characteristics that fall under prohibited bases (Swedloff, 2015). That is why removing sensitive attributes such as ethnicity and gender from databases is not practical when preventing the creation of discriminatory profiles (Kamiran & Calders, 2012).

For example, gender may be linked to whether a person works part-time or full-time, leading to a classifier that engages in indirect gender discrimination based on the type of employment contract. This would constitute indirect discrimination. Alternatively, property insurance companies may be biased toward charging higher property insurance premiums based on crime statistics. Since people of color are more likely to live in areas with higher crime rates, higher premiums based on crime rates are strongly correlated with race (Rubin, 2016).

Furthermore, it is often assumed that big data algorithms make objective judgments. Contrary to this belief, algorithms often contain hidden biases that can lead to discriminatory outcomes. For example, a recruiting program might use an algorithm that learns from past hiring patterns. If these patterns are discriminatory, the algorithm will still learn them. As a result, discriminatory hiring practices may continue or even increase, often without internet users realizing it (O'Neil & Mann, 2016). Finally, the difficulty of imposing liability based on indirect discrimination is a typical obstacle in the fight against data-based discriminatory practices (Barocas & Selbst, 2016).

II.4. Control of Personal Data Under Article 11 of the EU Charter

According to article 11 of the EU Charter, freedom of speech is established as a fundamental human right, including the right to freely express opinions and the right to access information and ideas objectively, without interference from state agencies and without being limited by national borders (Peers, 2014). Nevertheless, freedom of speech is not only limited to speech, but also includes other forms of expression, such as art, journalism, and digital media. Freedom of speech includes (i) the right to express opinions, views, and information freely; and (ii) the right to receive information in a complete, objective, and diverse manner, contributing to the formation of individual awareness and decisions (Peers, 2014).

In the context of the digital age, with the strong development of information and communication technologies (ICTs), freedom of speech has been reduced due to the "information restriction effect". It is the change in behavior of individuals when they are aware that they are being monitored, leading to individuals limiting the expression of their opinions. Likewise, surveillance can be carried out by many different subjects, such as (i) surveillance by competent state agencies to ensure national security, public order, or crime prevention; (ii) surveillance by organizations and individuals for commercial purposes, to protect private interests, or to monitor the behavior of others; and (iii) use of technology to collect and analyze data like social media surveillance, location tracking, or facial recognition. In that sense, surveillance aims to ensure compliance with the law, ensure security, or optimize business operations. However, surveillance also limits freedom of expression, self-

censorship in individual behavior, and the decline of public space for exchange and debate (Bachlechner, 2015).

Regarding this, the CJEU has recognized the negative impact of surveillance on human rights, particularly the right to privacy and freedom of expression. The CJEU has made several important judgments to protect these rights against online surveillance, such as tracking users' behavior, information, and interactions on the internet, social networks, and other digital platforms to collect and analyze information about users (search history, location, financial information, etc.). In the Digital Rights Ireland case, the Court stated: "First of all, it must not be overlooked that the sense of uncertainty about surveillance can have a decisive influence on European citizens' exercise of their right to freedom of expression and information, and thus interference with the right guaranteed by article 11 of the Charter may also occur".

Additionally, the right to freedom of expression under article 11 of the EU Charter is the right to express opinions and receive information thoroughly and objectively (Peers, 2014). With the popularity of the internet, the right to receive information is becoming increasingly important. Google's personalization of results can lead to information "filter bubbles", limiting users' access to diverse and objective views (Hannák, 2013). Also, Google's behavior violates the right to receive information and, therefore, the right to freedom of expression. Specifically, Google's PageRank algorithm predicts the interests and behavior of internet users, which can lead to users only having access to information that suits their interests, thereby ignoring diverse and objective views (Pariser, 2011). Finally, algorithms can also be used to manipulate information for political or commercial purposes (European Data Protection Supervisor, 2015).

Therefore, there is a need for appropriate policies to govern search engines, such as requirements for algorithmic transparency and personalization of search results and diversity and objectivity of search results to ensure the right to information of internet users. Finally, search engines and some companies have developed complex governance mechanisms to regulate speech and expression online (Klonick, 2018); however, their governance systems face significant problems, as they are often arbitrary, non-transparent, and can be abolished whenever necessary or convenient (Balkin, 2018).

According to the aforementioned, in 2018, the EU launched an initiative on hate speech, requiring platforms to establish a system that allows for the immediate removal and monitoring of content that resembles hate speech. It was evident that reducing interference in platforms and increasing transparency for internet users is necessary to ensure the privacy of internet users, as stipulated in article 11 of the Charter.

III. CONCLUSION

III.1. Develop Vietnamese Law on Personal Data Protection in Technology-Neutral Language

Personal data protection must be technology-neutral, regardless of the algorithms used. Kamara (2018) argues: "Laws that are technology-specific will inevitably become obsolete or will create legal gaps by regulating some existing technologies that will no longer be suitable for algorithms and technologies that develop in the future" (p. 10). Therefore, the essence of technology-neutral law is that it does not discriminate between technologies if the *raison d'être* of the

law applies equally to all technologies, whether present or future. Reed (2017) argues: "Technology-neutral regulation has three main goals: ensuring the future, not distinguishing between online and offline, and encouraging the development and adoption of new technologies" (p. 10).

When it comes to the digital economy, technology-neutral language will ensure that Vietnamese data protection laws do not become obsolete as technology advances and do not favor certain technologies over others, which would limit technological innovation and business freedom (Reed, 2017). Therefore, it is important to note that the EU data protection regime was drafted with the principle of technology neutrality in mind from the outset. In other words, the technology neutrality of personal data protection laws also helps ensure that the digital economy's development is not hindered by cumbersome procedures (Scholz, 2017).

III.2. Vietnamese Law Needs to Promulgate a Regulation Explaining the Term *Personal Data*

Vietnamese law on personal data protection must clearly explain the term *personal data*. This includes not only information that can be linked or associated with a specific individual at the time of data processing, but also all information that can be linked or associated with that individual during future processing, possibly by technological means that have not yet been developed at the time the personal data is collected or created.

According to this, current data that is not considered personal data may become personal at some point. The law on personal data protection needs to consider all objective factors, such as the cost and the amount of time required

for identification, and the technology available at the time of personal data processing and future technology developments.

The increased use of linked, combined, and blended data also widens the ambiguous boundary between personal and non-personal data (Bart van der Sloot, 2014). Data that appears anonymous today may become personal data through future technologies beyond the data subjects' control. In the future, the likelihood that anonymous data will be re-identified or linked to an individual will increase exponentially as more data is exploited for commercial purposes. Bart van der Sloot (2014) argues: "The non-exhaustive list of possible identifiers for personal data reflects that data that at one point in time may not contain information about a specific individual may be used through advanced techniques to identify or personalize a person" (p. 10).

> Furthermore, even data that does not identify a person may increasingly be linked, among other means through connection and database collection, and used to create profiles so that two or more sets of anonymous data may become identifiable data sets. (European Commission, 2016, p. 1)

Finally, data that is not directly linked to a person may still be personal data if it can be linked to a specific person when combined with additional data that may be held by parties other than the data controller (European Commission, 2016). However, not all data must be considered potentially identifiable, and reasonableness must also be considered (European Commission, 2016). The assessment of reasonableness should take into account the state of the art at the time of processing and the likely developments over

the period during which the data will be processed (European Commission, 2016) and should be interpreted flexibly, depending on the specific circumstances (European Commission, 2016).

REFERENCES

Balkin, J. (2018). Free Speech Is a Triangle. Columbia Law Review, 118(7). https://columbialawreview.org/content/free-speech-is-a-triangle/.

Barocas, S., & Selbst, A. (2016). Big Data's Disparate Impact. California law review, 671, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.

Beitz, C. (2009). The Idea of Human Rights. Oxford University Press.

Bosco, F. (2015). Reforming European Data Protection Law . Springer.

De Hert, P., & Gutwirth, S. (2006). Privacy and the criminal law . Intesentia.

De Hert, P., & Gutwirth, S. (2009). Reinventing Data Protection? . Springer.

European Commission. (2016). How Does the Data Protection Reform Strengthen Citizens' Rights? etc.europa.eu/newsroom/just/document.cfm?doc_id=41525

Hijmans, H. (2016). The European Union as a Constitutional Guardian of Internet Privacy and Data Protection. University of Amsterdam.

Hornung, G., & Schnabel, C. (2009). Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination. Computer Law and Security Review, 25(1), 84-88. http://dx.doi.org/10.1016/j.clsr.2008.11.002.

Hustinx, P. (2015). EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf

Klonick, K. (2018). The New Governors: The People, Rules, And Processes Governing Online Speech. Harvard Law Review, 131, https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf.

Kokott, J., & 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). /https://portal.ejtn.eu/PageFiles/19789/J.Kokott%20and%20C.%20Sobotta%20The%20distinction%20between%20privacy%20and%20data%20protection%20in%20the%20jurisprudence%20of%20the%20CJEU%20and%20the%20ECtHR.pdf.

Koops, B. (2016). A Typology of Privacy. University of Pennsylvania Journal of International Law.

Lynskey, O. (2015). The Foundations of EU Data Protection Law. Oxford University Press.

McDermott, Y. (2017). Conceptualización del derecho a la protección de datos en la era del Big Data. Big Data & Society , 4 (1). https://doi.org/10.1177/2053951716686994.

Middelaar, L. (2013). The Passage to Europe: How a Continent Became a Union. Yale University Press.

O'Neil, C., & Mann, G. (2016). Hiring Algorithms Are Not Neutral. Harvard Business Review: https://hbr.org/2016/12/hiring-algorithms-are-not-neutral

Pariser, E. (2011). The Filter Bubble: What the Internet Is Hiding from You. Penguin Press.

Peers, S. (2014). The EU Charter of Fundamental Rights: A Commentary . Hart.

Quane, H. (2012). A Further Dimension to the Interdependence and Indivisibility of Human Rights: Recent Concerning the Rights of Indigenous Peoples. Harvard Human Rights Journal, 25, 50. https://journals.law.harvard.edu/hrj/wp-content/uploads/sites/83/2009/09/Quane.pdf.

Solove, D. (2002). Conceptualizing Privacy. California Law Review.

Stilman, G. (2015). The Right to Our Personal Memories: Informational Self-determination and the Right to Record and Disclose Our Personal Data. Journal of Ethics and Emerging Technologies, 25(2), 14-24. https://doi.org/10.55613/jeet.v25i2.45.

Swedloff, R. (2015). Risk Classification's Big Data Revolution. Connecticut Insurance Law Journal, 21, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566594.

Watson, P., & Ellis, E. (2012). EU Anti-Discrimination Law. Oxford University Press.

Westin, A. (2015). Privacy and Freedom. Ig Publishing.