Eksplorium *p*-ISSN 0854-1418
Volume 46 No. 1, May 2025: 698–711 *e*-ISSN 2503-426X

Study on the Right to Access Under GDPR to Recommend Policy for Vietnam on Personal Data Protection

Dr. Vo Trung Hau
Binh Duong University, Vietnam
vthau@bdu.edu.vn
ORCID: 0009-0006-3560-4359

Article Received: 22 Feb 2025, Revised: 25 April 2025, Accepted:07 May 2025

Abstract: The right to access is one of the control rights and represents an important element in enhancing users' control over personal data. The goal of the right to access is to provide comprehensive access to data about an individual's use of a service in a convenient, secure, private and free manner. This article introduces the content of the right to access under the General Data Protection Regulation (GDPR), including the right to access anonymised data, the right to access shared data, linked databases, the right to access information about automated decision-making and exceptions to the right to access. From there, the article summarises and provides directions for improving Vietnamese law on personal data protection related to the right to access.

Keywords: Right of access, personal data, personal data protection

1. INTRODUCTION

When clarifying the disclosure of personal data to third parties, the European Court of Justice (CJEU) has drawn a close connection between the exercise of the right of access and the fundamental values of privacy: "*Privacy means that the data subject can be sure that his data are processed correctly and lawfully, in particular, that the basic data concerning him are accurate and disclosed to those authorised to receive them. To carry out the necessary checks, the data subject must have access to the data concerning him."* [1] The right of access is one of the rights of control and represents an important element in enhancing user control over personal data[2]. The goal of the right of access is to provide comprehensive access to data about an individual's use of the service in a convenient, secure, private and free manner[3].

The right to access personal data has been included in all data protection mechanisms in many countries worldwide.[4] and became the basis of data protection law to this day[5]. The right of access is considered part of the Charter of Fundamental Rights of the European Union (CFR). Furthermore, the importance of access is confirmed by the fact that strengthening the rights of data subjects was one of the core objectives of the European General Data Protection Regulation (GDPR). In the United States, Alan Westin argues that the constitutional principle of due process

[1]Case C- 553/07 Rijkeboer, para. 49.

[2] European Commission (2010), " Communication from the Commission to the European Parliament, the Council, the Economy and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union ", page 7.

[3]Fischer-Hübner S et al. (2013), Digital Enlightenment Yearbook 2013, IOS Press, p. 133.

[4]Colin J Bennett (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, page 106.

[5] Anupam Chander, Margot E Kaminski and William McGeveran (2019), Catalyzing Privacy Law, Minnesota Law Review.

should apply to the processing of personal data. [6]. In this view, the right to access personal data is essential to protect due process. For Westin, access is not aimed at protecting "*privacy as control* ". Instead, Westin develops the idea that people should have the right to access data to protect their "*due process" rights* in the age of electronic data processing[7]. Alan F. Westin defines the concept of "*privacy as control* " as " *the right of individuals, groups or organisations to decide for themselves when, how and to what extent information about them is communicated to others*."[8] This idea of " *privacy as control* " is considered a fundamental theory of personal data protection and privacy.

In the digital economy, data subject rights are often poorly respected. However, this assessment proceeds from a limited view of the place of the right of access within the broader data protection framework. The question is whether and how the right of access applies from a socially embedded perspective, considering the nature of the request method and the practical operation of the right of access. Does the right of access enable a person to usefully challenge decisions based on their data? Does the power asymmetry change in favour of the right holder due to the exercise of the right? [9]

2. CONTENT OF ACCESS RIGHTS ACCORDING TO THE GENERAL DATA PROTECTION REGULATION (GDPR)

2.1. Overview of access rights

The central requirement of "*privacy as control"* is that people should be able to decide when, how, and to what extent information about them is shared with others. Consent is a key principle associated with this vision.[10] The right to informational self-determination builds on that requirement. However, it acknowledges and emphasises that people often do not make decisions when and under what conditions information about themselves is communicated to others. Therefore, in all cases where data is communicated, people must be able to know who has access to their personal information and for what purposes it is used. For people to have this knowledge, the right to informational self-determination is based on the principles of transparency and purpose limitation. Therefore, "*privacy as control*" and "*informational self-determination"*.[11] Viviane Reding introduced the concept of informed consent, the right to data deletion where consent is revoked, and the right to data portability with the term "*empowering the individual to control their data"*.[12]

[6]Alan F Westin (2015). Privacy and Freedom , Ig Publishing, p. 54.

[7]Alan F Westin (2015). Privacy and Freedom , Ig Publishing, p. 54.

[8]Alan F Westin (2015). Privacy and Freedom, Ig Publishing, page 60.

[9]HU Vrabec (2019). Uncontrollable: Data Subject Rights and the Data-Driven Economy, Leiden University, page 63.

[10]Joris Van Hoboken (2019). The Privacy Disconnect, MIT Press, pp. 265-269.

[11]Hielke Hijmans (2016). European Union as guardian of Internet privacy: the story of Art 16 TFEU, Springer, p. 76.

[12]Viviane Reding (2012). The European Data Protection Framework for the Twenty-First Century, International Data Privacy Law, pp. 124–126.

Similarly, Orla Lynskey argues that data portability and the right to be forgotten promote information self-determination.[13] However, it is important to note that consent and data erasure gives people the right to decide when, how, and to what extent information about them is communicated to others. The right to control personal data is necessary to change the balance of power by creating the ability to evaluate and challenge individual decisions and decision-making systems. The object of control for "*privacy as control*" is personal data, while for "*informational autonomy*" it is the development of individual personality. Meanwhile, for "*due process"*, the main objects of control are the organisations involved in processing personal data, the decisions made, and the procedures applied. Information asymmetry is increasingly being noticed and is the subject of debate about data protection.[14]

Westin and Baker propose frameworks for data protection regulation that aim to provide a system of balance of power. Westin and Baker's view of the database is that the main concern is to protect civil liberties and prevent discrimination.[15] Meanwhile, the core of personal data protection is to prevent the concentration of power in the digital economy and ensure the free movement of data. Therefore, the balance of power is the rationale for data protection and the main reason for the existence of the General Data Protection Regulation (GDPR). Freedom and autonomy develop when people turn their attention to the individual. With the development of sociology, subjectivity is introduced in the definition of fundamental rights when individuals should have the right to know and control what data is stored about them to ensure the free development of the individual. Article 15 of the General Data Protection Regulation (GDPR) provides for the right of access, which provides data subjects with the following three rights. First, the right of access provides data subjects with the right to receive information about whether or not their data is being processed. Second, the right of access allows individuals to be informed about the nature of the data processing. This additional information must be provided in an easily understandable form; it must include the purposes of the processing, the categories of data concerned, the recipients or a list of recipients to whom the data is disclosed, the retention period, the existence of certain other rights, information about the source if the data was not collected from the data subject, and any information available about the source and logic involved in any automated data processing.[16] This right also allows data subjects to have access to their data by receiving a copy of the data being processed.[17]

An individual's right to be confirmed that information about him or her is being processed is often understood to mean that the controller must respond to any request, even if the response is to deny that the data is being processed.[18] The right of access allows individuals to check whether their

[13]Orla Lynskey (2014). Deconstructing Data Protection: The " Added-Value " of a Right to Data Protection in the EU Legal Order, International and Comparative Law Quarterly, page 132.

[14]Damian Clifford, Inge Graef & Peggy Valcke (2018). " Pre-Formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections ", German Law Journal, page 679.

[15]Alan F Westin & Michael A Baker (1972). Databanks in a Free Society, Quadrangle Books, pp. 3 20.

[16]Article 15 General Data Protection Regulation (GDPR).

[17]Article 15 General Data Protection Regulation (GDPR).

[18]Eduardo Ustaran et al. (2012). European Privacy: Law and Practice for Data Protection Professionals, International Association of Privacy Professionals, page 127.

data is being processed. This is an important point in the digital economy, given the widespread practice of sharing and reusing data that leaves consumers unclear about the location and flow of their data. For example, some people who are not Facebook members still use Facebook's public pages when they browse other websites. Facebook also processes the personal data of these people as IP addresses.[19] The right of access also allows unregistered users to check whether and how their data is processed. This will increase data subject control and make access more effective as it will no longer be necessary to restrict access to frequent service users unreasonably.

Compared to the Data Protection Directive (DPD), the information provided to the data subject under the right of access of the General Data Protection Regulation (GDPR) is more extensive; it includes references to supervisory authorities, information on the right of control and information on third-party sources of information. In particular, more and more information is collected not from the data subject but through intermediaries and other third parties. In addition, the provision relating to information on automated decision-making has been expanded to include information on the significance and possible consequences of data processing for the data subject.

Facebook collected user data based on their consent. This data was then shared with a third-party application based on public interest research. The legal basis for the research is unlawful, as the ultimate use of the data was commercial rather than scientific.[20] However, not being able to access information about the legal basis would be of much use to the data subject. While this information may shed light on potentially problematic uses of the data, it is not feasible for the data subject to effectively monitor the use of the data in this way. Furthermore, Facebook recently disclosed that it works with over 90 million third-party applications.[21] Providing this information would impose a large, and even disproportionate, burden on data controllers.

In principle, the right of access provides data subjects with a wide range of information, which should give them more control. However, there are some limitations to how the right of access can be applied in practice. Providing copies of personal data in a data-intensive digital economy can be difficult for several reasons. First, the right of access does not apply to anonymised data, although anonymised data is widely used in the digital economy and can have several consequences for individuals. Second, data is often pooled or a shared resource. Both of these facts complicate the application of the right of access. Finally, the right of access can be used to monitor algorithmic decisions, but the extent to which this can be done remains controversial.

2.2. Access to anonymous data

According to Article 15 of the General Data Protection Regulation (GDPR), the data subject can access personal data. This means that before granting access, the controller must clarify whether

[19]Gennie Gebhart (2018). "Facebook, This is not what "complete user control." looks like", https://www.eff.org/deeplinks/2018/04/facebook-not-what-complete-user-control-looks

[20]Carole Cadwalladr and Emma Graham-Harrison (2018), How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool, The Guardian https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm

[21]Brittany Darwell (2012). The Facebook platform supports more than 42 million pages and 9 million apps, Adweek.com http://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps/

the data requested falls within the definition of personal data. Determining the exact scope of the right of access becomes difficult due to the unclear boundaries of the concept of personal data.[22] For security and convenience reasons, companies that operate on data often use anonymised data. Anonymised data is considered non-personal because the identifying elements can lead to an individual being removed from the data set. Data protection law focuses on individuals who have been identified or identifiable, so in the case of anonymised data, data protection law cannot apply. Similarly, an individual cannot apply for access to check his or her data after removing the identifying elements.

However, anonymising personal data is not always an effective solution to protecting privacy. Anonymised data sets can often be as useful as personal data and have similar negative consequences for individual privacy. While user identities are effectively protected when each data set is collected independently, certain individuals can still be re-identified by aggregating data from multiple sources into a large data set to find new patterns and correlations.[23] In other words, identifying individuals from anonymised data is becoming increasingly easy.[24] Computer scientists have demonstrated that anonymisation techniques can fail by developing algorithms that can turn anonymised data into names and addresses.[25] This does not mean data anonymisation should be abandoned, but it is a useful reminder that anonymising personal data is an imperfect privacy protection technique.[26] Moreover, the negative consequences can extend beyond privacy invasion. If someone wants to exercise their right of access, the controller must determine the identity of the person requesting access. This becomes difficult when it comes to accessing data about unidentified individuals.[27] The gap between anonymous and personal data concerns data where certain identifying elements are transferred so they can no longer be attributed to the data subject.[28] For example, today, online services can use unique identifiers to track individuals without being

[22]E Brouwer and F Borgesius Zuiderveen (2015). Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU 's YS. and M. and S. Judgment (C-141/12 and C-372/12), European Journal of Migration and Law, page 6 8.

[23]Primavera De Filippi (2014). Big Data, Big Responsibilities, Internet Policy Review, page 4.

[24]Ohm P (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, p. 1701.

[25]Narayanan A and Shmatikov V (2009). De-Anonymizing Social Networks, IEEE Symposium on Security and Privacy.

[26]Ohm P (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, p. 1699.

[27]Zwenne GJ (2013), Diluted Privacy Law, Universiteit Leiden, https://hdl.handle.net/1887/24916

[28] Runshan Hu et al. (2017). Data Protection and Privacy: The Age of Intelligent Machines, Hart Publishing, p. 35.

able to identify the user.[29] This often happens as part of online behavioural advertising[30]. Should an individual know that they have received an advertisement because an analysis of their profile indicates a personal characteristic?[31] Some scholars argue that they should know because whenever data is used to distinguish someone, this should be considered personal data processing. Such an interpretation is also consistent with the General Data Protection Regulation (GDPR) view of profiling, where any use of data, including personal information, to predict someone's preferences is considered personal data processing.[32]

Anonymised data is processed so that it cannot identify or identify a particular individual.[33] Whether the right of access applies to anonymised data is not yet clear. Article 11 of the General Data Protection Regulation (GDPR) provides the following: "*If the controller can demonstrate that it is unable to identify the data subject, Articles 15 to 20 shall not apply unless the data subject, to exercise his or her rights under those articles, provides additional information that allows him or her to be identified".* Therefore, if the data subject exercises his or her rights under Articles 15 to 20 of The General Data Protection Regulation (GDPR), which provides additional information that allows identification of oneself, will apply the right of access.

However, requiring individuals to establish evidence of personal data can be a significant burden given their lack of expertise and the powerful influence of application platforms. Cohen notes that consumer personal data is often deeply embedded in the operating protocols of mobile platforms or web browsers and can involve complex commercial relationships between multiple participants in the platform's cross-licensing ecosystem. Platforms lead the way: "*The complexity and opacity of platform companies suggest that traditional approaches to identifying personal data are inadequate to the delicate balance between powerful platforms and vulnerable users."*[34]

2.3. Access to shared data, linked databases

Two distinct data characteristics make it difficult to apply the full scope of Article 15 of the General Data Protection Regulation (GDPR) because data is a shared resource. And data are often combined. As a shared resource, access to one person's data can infringe on the privacy of others. Advances in data processing techniques mean that personal data is no longer purely personal. Article 15 of the General Data Protection Regulation (GDPR) stipulates that exercising the right

[29]European Parliament (2013). Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and on the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs (LIBE), http://www.europarl.europa.eu/cmsdata/59696/att_20140306ATT80606-4492192886392847893.pdf

[30]Sophie Stalla-Bourdillon and Alison Knight (2017), Anonymous Data v. Personal Data - a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Review, page 285.

[31]Josh Constine (2015). Facebook Finally Lets Its Firehose Be Tapped For Marketing Insights Thanks To DataSift, TechCrunch, https://techcrunch.com/2015/03/10/facebook-topic-data/

[32] Article 4 General Data Protection Regulation (GDPR).

[33]Article 4, Clause 4 of the General Data Protection Regulation (GDPR).

[34]Cohen JE (2017). Law for the Platform Economy, UC Davis Law Review, p. 133

of access must not adversely affect the rights of others.[35] A similar situation occurs when accessing social network data: a user's contact list also includes much information about those contacts' profiles and online activities. Furthermore, data is often shared and reused by third parties during processing. The GDPR requires the controller to inform the individual about those recipients, but it is not the controller's obligation to facilitate access to this information. Instead, the data subject should turn to the secondary data controller with a new request.[36]

However, the primary controller must allow access to third-party information that has been combined with its data and is still being used on its premises. For example, in its privacy policy, LinkedIn states that data from data aggregators is combined with LinkedIn's data and used for online behavioural advertising purposes.[37] However, a request for access to LinkedIn only results in receiving a limited set of information without any indication of how the data is combined and how the user's profile is enhanced. Since these activities are core to LinkedIn's commercial strategy, it is reasonable for an individual to have some insight into the mechanisms by which their data is processed. The above cases demonstrate that specific data characteristics result in limited access effectiveness. Access may be restricted or denied when a data set includes information about third parties. Similarly, once data has been shared or reused with third parties, access to the data becomes more difficult or even impossible. Since the General Data Protection Regulation (GDPR) does not change the fundamental content of the right of access, while data processing is becoming increasingly complex and uncontrollable, the right of access may be affected in the future due to the inability to address changes in the digital economy.

2.4. Right to access information about automated decision-making

Although the Data Protection Directive (DPD) version of the right of access has been carried over to the General Data Protection Regulation (GDPR) without any major changes, the scope of the right of access has been expanded in some respects. Article 15 of the GDPR states that the response to an access request must also provide information about the logic, intended outcome, and the significance of automated decision-making. In practice, this small change is significant. Veale and Edwards claim this additional information is the G DPR's most powerful weapon against data-driven, algorithmic manipulation.[38] Specifically, the need for transparency in automated decision-making is high in the digital economy. Even routine operations now involve complex decisions that computers make, as everything from cars to home appliances routinely incorporate programming code into their normal operations.[39]

However, access to data, including explanations, will only be possible when the buyer's data is factored into the algorithms.[40] Access cannot be applied if a company calculates a score without using personal data. Does this mean that price discrimination is not possible? Philip Hacker and

[35]Paragraph 63 General Data Protection Regulation (GDPR).

[36] Information Commissioner Office, Subject Access Code of Practice, page 21, https://www.pdpjournals.com/docs/88115.pdf

[37]LinkedIn Privacy Policy https://www.linkedin.com/legal/privacy-policy

[38] Lilian Edwards & Michael Veale (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 24.

[39] Kroll et al. (2016). Accountable Algorithms, University of Pennsylvania Law Review, p. 50.

[40]Zuiderveen Borgesius FJ and Poort J (2017). Online Price Discrimination and EU Data Privacy Law, Journal of Consumer Policy, page 14.

Bilyana Petkova point out that Amazon has discriminated against online shoppers based on their laptop type, such as offering higher prices to MacBook users without including any personally identifiable data.[41] While such data processing may be a breach of personal data protection, access cannot be used to check data reuse.

Can the right to an explanation within the right of access framework be used to request an explanation of individual decisions that have been made based on personal data, or should it be limited to describing some basic system functions? It is important to note that access requests under Article 15 of the General Data Protection Regulation (GDPR) are typically made after data processing. Therefore, the data controller is required to provide the adjusted information after facts that have occurred about specific decisions that have been made about a specific data subject.[42] Such a solution seems reasonable and promises a right after the fact to be explained.[43] However, Wachter asserts that the right of access cannot be extended that far and that the provision's wording is too narrow to create any kind of right that could be equated with the right to an explanation.[44] Wachter argues that the right to an explanation is not what the legislators had in mind when drafting Article 15 of the General Data Protection Regulation (GDPR).[45] Although Michael Veale and Lilian Edwards acknowledge that the right to an explanation can be derived from the protections described in Article 22.3 of the General Data Protection Regulation (GDPR), they emphasise that the scope of this right is limited because it only applies to a narrow range of decisions “based solely on automated processing” and that have “legal effects” or “similarly significant effects” on the data subject. It can be seen that the right of access only provides “a general form of monitoring” and not “a right to an explanation of a specific decision."[46]

---

[41]Philip Hacker and Bilyana Petkova (2017). "Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers", Northwestern Journal of Technology and Intellectual Property, p. 13.

[42] Lilian Edwards & Michael Veale (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 34.

[43] Lilian Edwards & Michael Veale (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 34.

[44]Wachter, Mittelstadt and Florida (2017). Why a Right to Explanation of Automated Decision-Making
Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, page 5.

[45]Wachter, Mittelstadt & Floridi (2017). Why a Right to Explanation of Automated Decision-Making
Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, page 22.

[46] Michael Veale & Lilian Edwards (2018). Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, Computer Law & Security Review, page 399.

Given the urgent need to address the issue of algorithmic accountability, it should not be accepted the rejection of the idea of a right to an explanation of a particular decision.[47] The reference to national data sources is ineffective, given the novel and multinational nature of the General Data Protection Regulation (GDPR).[48] Furthermore, this right is already limited because non-personal data falls outside its scope, no matter how useful it might be in identifying people's preferences and vulnerabilities. Given the circumstances in which a lack of accountability for algorithms leads to unintended consequences, a broader interpretation seems more appropriate. Even if the proposed broader interpretation were to materialise, how the interpretation of algorithms in terms of the right to access could be implemented in practice or, other words.[49] What would the procedural steps for accessing information about algorithms entail?

2.5. Exceptions to access rights

The Data Protection Directive (DPD) allows national legislation to define the meaning of "a reasonable period" and "without undue delay or expense". This leads to differences between member states.[50] Under the General Data Protection Regulation (GDPR), member states' regulatory freedom in personal data protection is limited. The first copy of data must be free of charge, and subsequent copies may cost a reasonable fee under Article 15, paragraph 3 of the General Data Protection Regulation (GDPR). The GDPR's approach of lowering fees should encourage individuals to seek access. Surprisingly, despite being tech-savvy, some companies still traditionally approach access requests.

Under the General Data Protection Regulation (GDPR), remote access is the default option, especially for data-driven companies. Article 15.3 of the General Data Protection Regulation (GDPR) states that data subjects can make requests electronically and that, in principle, information will be provided in a commonly used electronic form. Paragraph 6.3, The General Data Protection Regulation (GDPR) provides some guidance on how to do this: *"Where possible, the controller must be able to provide remote access to a secure system that provides the data subject with direct access to their data." This is a reasona*ble requirement since personal information is increasingly processed online and in digital form. When a data-driven organisation implements a non-digital access process, users may point to dishonesty on the part of the organisation.

When does access take effect? In the case of Rijkerboer, The applicant requested access to information about all disclosures of his data to third parties from previous years.[51] What complicated things was that the requested data had been deleted under the retention restriction principle. In its judgment, the European Court of Justice (CJEU) weighed the data subject's interests in gaining access against the burden placed on the data controller in ensuring that personal data was available to the data subject. The court held that limiting the data to the recipient does

[47]Andrew Burt (2017), Is there a right to explain for machine learning in the GDPR, IAPP, https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/

[48] Yvonne McDermott (2017), Conceptualising the Right to Data Protection in an Era of Big Data, Journal of Foreign Legislation and Comparative Law.

[49]Aylin Caliskan, Joanna J Bryson & Arvind Narayanan (2017). Semantics Derived Automatically from Language Corpora Contains Human-like Biases, Science, page 45.

[50] Eduardo Ustaran et al. (2012). European Privacy: Law and Practice for Data Protection Professionals, International Association of Privacy Professionals Publishing House, p. 126.

[51]Case C- 553/07 Rijkeboer, para. 49.

not constitute a balance between the interests and the obligations under consideration unless it can be demonstrated that storing the information for a longer period would impose an undue burden on the data controller: "*In order to ensure the practical validity of the provisions on the right of access, the right must necessarily be retrospective. Otherwise, the data subject would not be able to effectively exercise his right to have the data alleged to be unlawful or inaccurate rectified, erased or blocked or to institute legal proceedings and obtain compensation for the damage suffered."*[52] The court noted that while the data relating to the transfer had been deleted, the underlying personal data had been retained for much longer. This mismatch was considered decisive in arguing that the retention of different data for the same period would not create an undue burden on the controller.[53]

The need to balance the interests of data subjects seeking access and those of data controllers seeking to protect data by providing less data is likely to increase. Some security design techniques that tend to eliminate the possibility of identifying personal data may conflict with data subjects' access and other rights. Finally, it seems reasonable that access may be restricted when requests are fraudulent. In practice, there is little that data controllers can do to prevent abuse of access. In principle, they cannot check the intentions of those requesting access or block access for improper intentions. Only under strict conditions can fraudulent requests be refused. The General Data Protection Regulation (GDPR) envisages an exception to the right of access to protect general public interests, such as public health and social security, under Article 23 of the General Data Protection Regulation (GDPR).

Another way to curb fraudulent access requests would be through Article 12, Clause 5. The General Data Protection Regulation (GDPR) prohibits requests that may adversely affect the rights and freedoms of others. Regarding abuse of rights, it is necessary to distinguish between the specific interactions between data-based forms of organisation and their users. It is difficult to imagine a situation where a platform such as Facebook, where data access requests are managed automatically, could claim misuse of access rights. Furthermore, data subjects are clearly at a disadvantage regarding platforms, making abuse even less likely. While traditional businesses may get into trouble if they receive too many requests, this is less likely to happen in the case of some modern forms of organisation. Exceptions to the right of access can be divided into two groups: (i) restrictions on the frequency of requests or the need to protect their privacy;[54] (ii) general exceptions apply to the entire category of control rights under Article 23 of the General Data Protection Regulation (GDPR). For example, access to certain data may be restricted for national security or public interest reasons.

3. POLICY RECOMMENDATIONS FOR VIETNAM

The General Data Protection Regulation (GDPR) explicitly requires that information regarding data access be provided in a "readily accessible and understandable format*, using clear and understandable language*." The U.S. government has mitigated the lack of transparency by replacing rankings with data that is publicly available and accessible on its website. *"The software*

[52]Case C- 553/07 Rijkeboer, para. 49.

[53]Anya Proops (2017), Yet another subject access judgment, https://panopticonblog.com/2017/03/06/yet-another-subject-access-judgment/

[54]Eduardo Ustaran et al. (2012). European Privacy: Law and Practice for Data Protection Professionals, International Association of Privacy Professionals, p. 127.

itself should be like an online website to create its user-controlled models of transparency"[55]. Another example of the successful implementation of data access rights tied to commercial services is access to online banking information.[56] Recent technological developments suggest that access rights may change in the future. Blockchain, which is a distributed database used to maintain a constantly growing list of records, can allow data subjects and trusted individuals easy, secure, and real-time access to personal data.[57] Blockchain will record someone's transactions or actions, such as doctor visits, and these records will be openly accessible. However, since not only the data subject but all other participants in the blockchain can access the same information, this can raise several other privacy issues.[58]

In addition, the digital economy is increasingly becoming a platform economy. The specific nature of platforms as non-transparent also adds to the problem. Access granted to individuals under the Data Protection Directive (DPD) is narrowly implemented.[59] Organisations provide individuals with little useful information while still complying with the law.[60] People are only granted access to some of the digital data they generate, much of which is not available to them because it is in the hands of Internet companies.[61] Since the DPA's access regulation is similar to the General Data Protection Regulation (GDPR), this trend will likely continue in the digital economy era. In that context, the author proposes some policy recommendations for Vietnam as follows:

Firstly, Vietnamese law needs to refer to the principles of the General Data Protection Regulation (GDPR) to develop a separate and comprehensive law on personal data protection with clear and detailed provisions on the right to access personal data in the context of the digital economy in Vietnam. In particular, Vietnamese law on personal data protection must clarify the scope, content and method of implementing the right to access. Specifically, Vietnamese law needs to stipulate the rights to (i) confirm the processing of personal data, (ii) access personal data being processed, (iii) provide information on the purpose of processing, type of data, data recipients, data storage time, right to edit, delete data, right to complain, data origin; (iv) receive a copy of personal data.

Second, Vietnamese law can refer to the General Data Protection Regulation (GDPR) to issue clear legal regulations on the obligations of data controllers in ensuring the right to access personal data, including (i) the obligation to provide information in a clear, understandable and accessible manner; (ii) the obligation to respond to access requests within the prescribed time limit; (iii) the obligation to verify the identity of the data subject before providing information. In addition, in

[55] O'Neil (2016), Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, page 30.

[56] European Data Protection Supervisor (2015). Meeting the Challenges of Big Data - A Call for Transparency, User Control, Data Protection by Design and Accountability, page 12.

[57]Molteni Megan (2017), Moving data is messy, but blockchain is here to help, Wired https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/

[58]Michèle Finck (2017), Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation & Competition Research Paper, page 23.

[59] Tene and Polonetsky (2013). Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, page 255.

[60] Tene and Polonetsky (2013). Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, page 255.

[61]Deborah Lupton (2015). Digital Sociologies, page 10.

order to ensure a balance between individual privacy and public interests, Vietnamese law needs to have provisions on exceptions to the right to access personal data for reasons of national security, public order, and protection of the rights and legitimate interests of others.

Third, Vietnam must issue policies that encourage individuals and organisations to apply technology. To ensure the protection of personal data and enforce the right of access. In the digital economy, privacy-enhancing technologies (PETs) use various methods, such as anonymous browsing or inserting "sounds" into data sets. Privacy-enhancing technologies (PETs) are: "*a coherent system of information and communication technology measures that protect privacy by removing or reducing personal data or preventing unnecessary or unwanted data processing*".[62] Accordingly, appropriate policy is needed to encourage the development of a range of technical measures to address the risks posed by advertising technology and to move towards less intrusive methods of tracking and profiling. Suggestions from Google and other market participants to phase out the use of " *third-party cookies*" and other forms of cross-site tracking and replace them with alternatives.[63] In addition, incentives are needed for individuals and organisations to adopt privacy-enhancing technologies (PETs) such as trust tokens, user agent minimisation, first-party datasets, federated group preferences (FloC), and federated group preferences (FLEDGE). The Global Privacy Control Framework (GPC) is a proposed technical solution that allows individuals to inform online services of their privacy preferences; it can be in the form of a browser setting or an extension that an individual can install. When enabled, GPC sends a signal communicating an individual's preferences about selling or sharing their data to each website.[64]

In addition, Vietnam could refer to the Information Commissioner's Office (ICO) proposal for "*identifiers"*; this proposal is based on some form of identifier, such as an email address.[65] The idea is that an email address is more anonymous and provides more privacy than an individual's name. Furthermore, Privacy Enhancing Technologies (PETs) are also developing several means for individuals to control their data, such as "*data vaults*", "*personal data archives"*, and "*personal clouds*."[66] Personal data archives can give individuals control over reusing their data across different services. This business model ensures that individuals deposit their data into these

[62] Commission (2007), Communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), page 228.

[63] Information Commissioner's Office (2021), Information Commissioner's Opinion: Data Protection and
privacy expectations for online advertising proposals, page 19.

[64] Information Commissioner's Office (2021), Information Commissioner's Opinion: Data Protection and
privacy expectations for online advertising proposals, page 2 6.

[65] Information Commissioner's Office (2021), Information Commissioner's Opinion: Data protection and
privacy expectations for online advertising proposals, page 27.

[66] European Union Agency for Network and Information Security (2015), privacprivacysign in big data: An
Overview of privacy-enhancing technologies in the era of big data analytics, pp. 47-48.

"*repositories*" that will manage the dissemination of the data according to the individuals' instructions.[67]

REFERENCES

[1]Case C- 553/07 Rijkeboer, para. 49.
[11]
[1].

1. Anupam Chander, Margot E Kaminski and William McGeveran (2019), Catalyzing Privacy Law, Minnesota Law Review.
2. Alan F Westin (2015). Privacy and Freedom , Ig Publishing, p. 54.
3. Aylin Caliskan, Joanna J Bryson & Arvind Narayanan (2017). Semantics Derived Automatically from Language Corpora Contains Human-like Biases, Science, page 45.
4. Anya Proops (2017), Yet another subject access judgment, https://panopticonblog.com/2017/03/06/yet-another-subject-access-judgment/
5. Andrew Burt (2017), Is there a right to explain for machine learning in the GDPR, IAPP, https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/
6. Brittany Darwell (2012). The Facebook platform supports more than 42 million pages and 9 million apps, Adweek.com http://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps/
7. Carole Cadwalladr and Emma Graham-Harrison (2018), How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool, The Guardian https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm
8. Cohen JE (2017). Law for the Platform Economy, UC Davis Law Review, p. 133
9. Colin J Bennett (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, page 106
10. Damian Clifford, Inge Graef & Peggy Valcke (2018). " Pre-Formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections ", German Law Journal, page 679.
11. Eduardo Ustaran et al. (2012). European Privacy: Law and Practice for Data Protection Professionals, International Association of Privacy Professionals, page 127.
12. E Brouwer and F Borgesius Zuiderveen (2015). Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU 's YS.
13. European Parliament (2013). Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and on the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs (LIBE), http://www.europarl.europa.eu/cmsdata/59696/att_20140306ATT80606-449219288639284789 3.pdf
14. European Commission (2010), "Communication from the Commission to the European Parliament, the Council, the Economy and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union", page 7.

[67] European Data Protection Supervisor (2015). " Towards a new digital ethics: Data, dignity and technology ", page 12.

15. European Data Protection Supervisor (2015). Meeting the Challenges of Big Data - A Call for Transparency, User Control, Data Protection by Design and Accountability, page 12.
16. European Union Agency for Network and Information Security (2015), privacprivacysign in big data: An
Overview of privacy-enhancing technologies in the era of big data analytics, pp. 47-48.
17. European Data Protection Supervisor (2015). " Towards a new digital ethics: Data, dignity and technology ", page 12.
18. Eduardo Ustaran et al. (2012). European Privacy: Law and Practice for Data Protection Professionals, International Association of Privacy Professionals, p. 127.
19. Fischer-Hübner S et al. (2013), Digital Enlightenment Yearbook 2013, IOS Press, p. 133.
20. Gennie Gebhart (2018). "Facebook, This is not what "complete user control."
21. HU Vrabec (2019). Uncontrollable: Data Subject Rights and the Data-Driven Economy, Leiden University, page 63.
22. Hielke Hijmans (2016). European Union as guardian of Internet privacy: the story of Art 16 TFEU, Springer, p. 76.

23. Lilian Edwards & Michael Veale (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 24.
24. Josh Constine (2015). Facebook Finally Lets Its Firehose Be Tapped For Marketing Insights Thanks To DataSift, TechCrunch, https://techcrunch.com/2015/03/10/facebook-topic-data/
25. Joris Van Hoboken (2019). The Privacy Disconnect, MIT Press, pp. 265-269.
26. Kroll et al. (2016). Accountable Algorithms, University of Pennsylvania Law Review, p. 50.
27. M. and S. Judgment (C-141/12 and C-372/12), European Journal of Migration and Law, page 6 8.
28. Michèle Finck (2017), Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation & Competition Research Paper, page 23.
29. Molteni Megan (2017), Moving data is messy, but blockchain is here to help, Wired.
30. Michael Veale & Lilian Edwards (2018). Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, Computer Law & Security Review, page 399.
31. Narayanan A and Shmatikov V (2009). De-Anonymizing Social Networks, IEEE Symposium on Security and Privacy
32. Ohm P (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, p. 1701.
33. O'Neil (2016), Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, page 30.
34. Primavera De Filippi (2014). Big Data, Big Responsibilities, Internet Policy Review, page 4.
35. Philip Hacker and Bilyana Petkova (2017). "Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers", Northwestern Journal of Technology and Intellectual Property, p. 13.
36. Runshan Hu et al. (2017). Data Protection and Privacy: The Age of Intelligent Machines, Hart Publishing, p. 35.

37. Sophie Stalla-Bourdillon and Alison Knight (2017), Anonymous Data v. Personal Data - a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Review, page 285.
38. Tene and Polonetsky (2013). Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, page 255.
39. Viviane Reding (2012). The European Data Protection Framework for the Twenty-First Century, International Data Privacy Law, pp. 124–126.
40. Yvonne McDermott (2017), Conceptualising the Right to Data Protection in an Era of Big Data, Journal of Foreign Legislation and Comparative Law.
41. Zuiderveen Borgesius FJ and Poort J (2017). Online Price Discrimination and EU Data Privacy Law, Journal of Consumer Policy, page 14.
42. Wachter, Mittelstadt and Florida (2017). Why a Right to Explanation of Automated Decision-Making