Exploring Cross-Jurisdictional Transfer of Digital Personal Data Protection Laws Using The Dignified Justice Theory

Teguh Prasetyo[1,] , *Faqi* Rawni Arndarnijariah[2*] , and *Jeferson* Kameo[2]

[1]Faculty of Law, Pelita Harapan University, Tangerang, Indonesia
[2]Faculty of Law, Satya Wacana Christian University, Salatiga, Indonesia

Abstract. This study discusses the legal vacuum and conflicting norms of digital data protection of individual citizens who use digital platforms transmitted trans-jurisdictions from European member countries to the United States. It comparatively reviews European Court decisions, European Directives, and Data Protection Laws as primary sources of law. The theory of Dignified Justice navigates the examination. It found that laws governing digital data transmission from one jurisdiction to another could be transferred to fill gaps and harmonize Indonesian law with European law in this area. Although in principle, according to the theory of Dignified Justice, the law must only be contained in the embodiment of the national spirit (*volkgeist*), among others, in existing regulations, especially in Indonesia or in the Pancasila Legal System, but through transposition according to the Dignified Justice Perspective it has been found that although there are differences in the formulation regarding legal norms protecting private digital data created to protect private digital data sent across jurisdictions, Indonesia also has substantive legal norms that are similar to the same law regime in Europe.

1 Introductions

Indonesia already enters and gradually leaving the revolutionary era of Industry 4.0. The revolutionary era is conceptualized as a cyber-physical system or the era of the digital revolution. Another characteristic of the digital revolution is the emergence of innovation and the new capacity to acquire, store, manipulate, and transmit volumes of data, especially personal digital data, in a real-time, comprehensive, and complex manner. Because of that, the digital revolution is often considered identical to the data revolution, namely the new era of data processing. According to law, data, including personal digital data [1,2], are tangible and valuable assets/objects or property (economic and others) because these data need protection from the law. However, one aspect of the arrangement about the protection of personal data, in this matter, is the arrangement law regarding the trans-jurisdiction transfer of personal digital data on the internet within one jurisdiction, especially in

* Corresponding author: rawniarndarnijariah@gmail.com

Indonesia, which must be reviewed to harmonize or transposed with rule law similar in other countries.

It is needed because the mentioned development of technology, information, and telecommunications has caused the world to become limitless (borderless). In the reality of the limitless world, the governing law that controls the limit of the passing activity must also be known in a manner that exists and adjusted or harmonized to be appropriately called as own rule law same quality anywhere activity has been done. Moreover, with the development of technology, information, and telecommunications that transverse the limit, there is also various type of change, for example, the change of social, economic, cultural, and so on, in a manner significant and accelerated fast. The need for laws protecting personal digital data from internet users is increasing following the development of the technology above. Man or subject law in various group ages nor corporations, including the state, is necessary subject law protected.

With great benefits for man in communication, the worldwide use of the internet is also followed with awareness of the need for protection law to user activity on the internet (online) because there is a digital footprint left behind, including personal digital data. Such awareness appears and increases among individuals of various group ages. [3] The same thing also arises from subject laws like corporations, including the state.

People (subject law) increasingly worry if digital footprints are left behind, and the personal digital data of internet users can be accessed, exchanged, and even manipulated, even by the power of data or party business internet platform manager without permission. [4] In the consciousness above, a person (subject law), whether individual human beings or corporations (incorporated or not) are concerned with protection law on personal data as internet users, including personal data protection from a company's interest toward digital platforms.

One of the Enterprise digital platforms is being targeted in the study, i.e., Facebook. Facebook is a social media and service network online social America owned by *Meta Platforms* and a network popular social used worldwide. Facebook has billions of active users. In guaranteeing the personal digital data of its users, Facebook already owns Standard Contract Clauses (SCC), some kind of bylaws.

The mentioned bylaws are already arranged when Facebook wants to transfer personal digital data users in that platform from one country or jurisdiction to another country or others (across jurisdictions). For example, this study highlights the personal digital data transfer case from the European Economic Area (EEA) to be processed in the United States or Third Countries, which is the main center of Facebook's operation. According to Facebook settings in SCCs, the goal of each data transfer, whether personal digital data between countries, is to provide a good service through the company according to Facebook Terms. Transferring personal data is meant to be helpful. According to SCCs, it is for Facebook to be able to operate and provide products globally to users. Thus, transferring personal digital data across jurisdictions' company digital platforms is an ensure technological activity.

The study's problem (legal issue) is that the internal settings from Facebook above conflict with the enforced common rule of law within one jurisdiction. As reviewed in this study, Facebook is conflicted with the rule of law of the states' members within the European Union. This is what it's called the law problem from this study, which is the existence of conflicting laws.

The mentioned conflict with the bylaws from Facebook above is the law that applies in the European Union community, namely the Data Protection Directive. The societal law in the European Union also contains laws governing the transfer of personal data from countries in the European Union to Third Countries. The term "to a third country" means "to the United States of America." It is also automatically projected in the study by personal

digital data of Facebook users in Indonesia. In the Data Protection Directive, the transfer of personal data can only be done if a third country (i.e., the United States) can ensure adequate data protection.

Formulated in Article 25 paragraph (1) Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals in connection with the processing of personal data and on the free movement of said data, that: transfers of personal data to third countries which are being processed or intended to be processed after transfers may occur only if, without prejudice to compliance with national provisions adopted under other provisions of this Directive, the third country concerned ensures an adequate level of protection."

According to the European Directive above, the adequate parameters from internal data protection formula provision law relate to all circumstances around data transfer or series data transfer operations. It needs to consider the data's nature, purpose, and duration of operation or processing operation proposed by the country of origin and destination end, rules of law, and whether it is general or enforces sectoral policies in third countries.

2 Method

The study uses the method of study law (legal research) [5] to find the rule of law or solution to the conflict in law above and also find the harmonization law that can be confirmed to fill the gap within the governing law of protection of transferred personal digital data in a manner trans-jurisdictions. The research law material within the study of law using approach comparison is directed to find a juridical solution, norm, or the rules contained within one decision court or case law, also in the European Directive, and its comparison with arrangement data protection in Indonesia. The referred law case within European Directive is the European Court's Decision or European Court of Justice (*Maximillian Schrems v Data Protection Commissioner*). It is essential to mention here that the European Court's Decision appears after the case in an authorized European court to check a decision from Personal Data Protection Commissioner, who previously saw a complaint from someone named Schrems.

The analysis in law research is done in a manner qualitative and deductive. The materials, such as the existing primary laws collected, are then classified by comparing the law approach (transposition) to search for the same meaning or relatively the same as the norm or regulation governing law protection of transferred personal digital data in a manner trans-jurisdictions.

Following the title of this research article, the findings are explored. In other words, the research is described, and so on, or analyzed using the Dignified Justice theory. The Dignified Justice theory holds a necessary postulate: the law is a system. The mentioned law system is the Pancasila law system.

It will be mentioned briefly here that according to or in perspective Dignified Justice theory, the norm law that, and with thereby must be understood including law norm that governs the protection of transmitted personal digital data in a manner trans-jurisdictions that already there within the nation's soul (*ubi societas ibi ius*). Pancasila is the soul of the nation (*volkgeist*), the source of all law's source. Pancasila is the value of law or supremacy of law.

Norm or the rule of law, part of system law, can be found in each manifestation of the nation's soul (*volkgeist)*. These manifestations of the nation's soul are the primary material law sources, For instance, applicable regulation, whether written or not.

Norm or the rule of law within one system of law, although seen similarly, the substances within them are not the same. It happens because each system of law has different beliefs and values. For that same reason also, it allows the Dignified Justice theory

to conduct a comparative study of law, or what is known as transposition, according to the Dignified Justice theory. Transposition is done to adapt, harmonize, or, more specifically, transpose beliefs and values around various system laws worldwide.

In the Dignified Justice theory, the possible transposition is intended to fill in the vacancy or vacuum of the meaning of values within the law (*rechtsvacuum*) that exist because the values or principles of law precipitate within the applicable law norm in one law system. Harmonizing beliefs and values in the law allow the enforceability of the norm or the rule of law in particular, including the allowing or justification of the norm's enforceability or certain rule of laws similar to various systems of law as guidelines of human behavior. With the existing guidelines, one can reach the objective of the law, the justice that humanizes humans (*nguwongke uwong*) as a creation of Almighty God, The Glorious One, within society. [6]

According to the Dignified Justice theory, if people will or want to find law, the law must be found through the soul nation (*volkgeist*). The concrete form or manifestation of *volkgeist* is an arrangement in Applicable Regulation laws and the court's judgments that legally bindings. As for the sought law in the study, it is a rule about norm protection of transmitted digital data to a third country from a Dignified Justice theory perspective.

As alluded to above, the Dignified Justice theory states that the law aims to humanize man as a creation of Almighty God (*nguwongke uwong*). The objective is not to antinomy between law objectives – justice, efficacy/utility, and certainty. So that according to this theory, every applicable regulation, as long as all of the applicable regulations, should apply as truth and is justice and efficacy and certainty of law (triad).

However, it is essential to know that Dignified Justice is not a concept of justice; instead, the meaning of Dignified Justice is a grand theory of law. The Dignified Justice function is to explain and justify something system applicable law. The Dignified Justice theory elaborates and justifies a system of law, including one rule or norm in the legal system with postulates, for example, that law exists and grows in soul nation or *volkgeist.* [7]

The Dignified Justice theory holds on to the postulates that law is one system that works to reach the purpose of Dignified Justice or justice that humanizes humans. Justice is everyone's spiritual needs and is an adhesive of social relationships in the state, and the court is the main pillar of law and justice enforcement as well as in the development process of a civilized nation. The enforcement of law and justice, as well as the respect for the nobility of human values, is the preconditioning of the uprightness of the dignity and integrity of the State. [8]

Aligning with the perspective of Dignified Justice theory, the analysis by the writers uses the comparative study of law. The writers view that the norms used by judges in European decisions (*a quo)* are explored possess the equivalent or similarity in a manner substance though cumulatively different from norms in Indonesia.

3 Discussion and Analysis

Before starting the discussion and analysis in this part, it will start with the findings about laws' arrangement that governs the transfer of personal digital data in a manner trans-jurisdictions that contains within the primary law's materials of this research. The findings or results study in the law case is about the problem of a Complainant named Schrems.

Schrems questions Facebook's action as a digital platform company (data power) that has treated personal digital data owned by Facebook as opposed to the law. His data is not handled according to applicable laws established by Schrems in the European Union. Facebook transfers his data from the European Union (Ireland) to a third country (jurisdiction), the United States (Maximilian Schrems v Data Protection Commissioner,

joined party: Digital Rights Ireland Ltd., Judgment of the Court of Justice of 6 October 2015 in Case C-362/14. n.d.).

However, according to Schrems, personal digital data transfer is opposed to the law or not fulfilling the provision of the European Directive, as stated above. It is important to know that Schrems is an Austrian citizen incorporated within the European Union. Because of that, the mentioned Directive is also applicable to protect the rights of Schrems as a user of information technology that links with telecommunications technology, often called internet technology.

Schrems, or Maximillian Schrems, is a Facebook user in the European Union. He submits the complaints to the Ireland Commission of Personal Data Protection. Ireland is a country that is also considered part of the European Union. Schrems' complaint states that Facebook, a company that operates in Ireland Ltd (Facebook Ireland), transfers his personal data to the United States. Initially, personal data Schrems stored on Facebook servers located in Ireland.

Schrems complained that the United States does not give a sufficient guarantee of protection for his data. Remembering personal data, the original Schrems was on Facebook Ireland, then transmitted to Facebook United States, got accessed by authorities public in the United States who carry out function supervision according to the law in the United States.

At first, all of Schrems' lawsuits were rejected by Ireland's Commission on Personal Data Protection. According to Safe Harbor Privacy Principles or Safe Harbor Agreement United States, or what is mentioned above as bylaws, the Commission's thoughts already ensure the protection of transmitted personal data. On the contrary, according to the European Court's judgment, Safe Harbor Privacy Principles, Safe Harbor Agreement, or Bylaws did not protect transmitted personal data from Ireland to the United States as a Third Country. The European Union Court stated Safe Harbor Agreement used by Facebook to defend itself is a nonvalid agreement.

3.1 Filling the Lacunae Juridical Meaning of Arrangement Personal Digital Data Protector

As stated above, the same problem in the study is the vacancy of law (*rechtsvacuum* or *lacunae, gaps*) in Indonesia. The meaning of the law's vacancy is that no particular meaning can be made about juridical (rules) in understanding arrangements to protect transmitted personal digital data trans-jurisdictionally. It says so because if Facebook uses Safe Harbor Privacy Principles or Safe Harbor Agreement (Bylaw) to defend itself in Court Europe, as pictured above, it is stated that it does not ensure the data's protection, which is invalid. Then the same thing also happens in Indonesia since there is no protection of personal digital data from Facebook users in Indonesia. At least, as stated above, there is no clarification of the meaning (*lacunae*) of whether the appropriate regime of data protection that applies, such as the PDP Law, has the same institution as the Data Protection Commissioner.

If compared to what happened with Schrems in Ireland, then in Indonesia, it can be stated here as not yet, or there is no clear juridical meaning that can be installed in a similar case. So, there should be a *rechtsvacuum* set to protect individual/corporation owners of personal digital data Facebook users stored on Facebook Indonesia, which Facebook Indonesia transmits to the United States and to be processed there.

Following the logical way of thinking as described above, after personal data (digital) of Indonesian Facebook users arrive on Facebook United States, it is clear that personal data experience the same treatment in Schrems's case, which is the data can be seen by the

supervisors in the United States. As a result, the value of proper personal data protection inside the law disappears.

Based on that claim, it can be said that there is a problem in Indonesian law, which can be interpreted as a violation of the law on personal digital data protection in Indonesia. According to the Act of PDP, violations done to Facebook users in Indonesia should be submitted to Indonesian law.

The precedent in *Maximillian Schrems* v. *Data Protection Commissioner* in the European Union, although not part of Indonesian law, can be used or transposed into law protection of personal digital data internet users in Indonesia. At least presented in the European Union in the case law *Maximillian Schrems* v. *Data Protection Commissioner* can be seen its possible chances of norms or the rule of law that will also happen in Indonesia, for example, to understand the Data Protection Act.

Case Law *Maximillian Schrems* v. *Data Protection Commissioner* can be used by the harmed Facebook users in Indonesia due to the same experience as Schrems above. Because of that, based on the meanings described above, according to this article's writers, the problem of law's vacancy *(rechtsvacuum*) can be overcome by taking a meaning (the rule of law) that existed or formed in the *Maximillian Schrems* v. *Data Protection Commissioner)*.

3.2 Human Rights Protection in the Shape of Arrangement Personal Digital Data Protector

Indonesia is a rule-of-law country. The legal basis is evident in Article 3 Paragraph (1) of the Constitution of the Republic of Indonesia (The 1945 Constitution of the Republic of Indonesia). A characteristic of the law's norm should exist in the state law concept. The particular characteristic should exist in the principle of the rule, which derives from Pancasila, which is, essentially, not the same as the laws that apply in the West. In a state of Pancasila law, it has been acknowledged that there is law sovereignty and its derivation from Pancasila. [9] In Dignified Justice theory, which is the purest theory of Indonesian people's law and was invented and designed with excavated materials from the archipelago by children of the Indonesian nation, determines that if there are conflicting laws with the highest Indonesian nation (Pancasila as supreme law/the rule of law), then it cannot be called as a law.

Based on the rule of law, no moral and ethical values exist beyond the law. For example, there is no moral inside the allowed political law in a manner of juridical to govern, control as well as natural laws and regulate the applicable regulations. Unless, for moral and ethical values that are already first "put" into law or customized with the values inside the law, the matter is with law, namely in Pancasila as the supremacy of law. The critical thing to notice in the context of democratic principles of constitutional-related human rights is the transformation of human rights from natural to constitutional. In other words, the value of Human Rights is "inserted" into law. The transformation of human rights from natural rights to constitutional rights is through the Second Amendment of The Constitution of the Republic of Indonesia (1945 Constitution of the Republic of Indonesia). [10]

The transformation of human rights to the constitution's characteristics, such as declarative and then give protection. The protection of human rights in the law's state, embodied in the form of normalization of rights in the constitution, the law, and the next one is the enforcement through the judiciary as executor strength judiciary.

If the discussion concerns the law's state and basic human rights, the state should have an obligation to honour, protect and fulfill them. In *a contrario,* it states that the violation of

human rights is the act or non-act by the conflicting state with the obligation of its human rights, which is to honour, protect or fulfill.

The characteristic of the rule of law concept is that there is nothing, and nobody can be equal even higher than the law. It also explains that all the orders in life, nation, society, and state are based on applicable law. This is aligned with the meaning of Indonesia as the rule of law stated in Article 1, paragraph (3) of the 1945 Constitution. If it is reviewed in the European Court's Decision, the European Union has the rule of law where all actions of its institutions submit to its suitability review. It is included within the agreement, principles of general law, and applicable basic rights in the European Union.

It is described above that in Indonesia, and the European Union, the related rule of law concepts have similarities and differences in significant matters. In Indonesia, all orders from its people until high officials should be submitted to applicable law in Indonesia. In other meaning, the law means the arrangement of applicable regulations. While the rule of law states that there is nothing and nobody is equal is even higher than the law. The European Union means that all member states must be subjected to the rules that have been approved together and applied universally in the European Union.

Then, the European Union applies written law in Directive 95/46 to protect personal digital data. So, everyone or all existing orders in the European Union must be submitted to law or regulation when speaking about protecting personal data and movements of the data.

Furthermore, the link between the concept of the rule of law and the rights of human rights, the state should respect, protect and fulfill the rights of its people. The statement that the state cannot create or make human rights with law or invention, and "*the role of the State is nothing more than declarative,"* so that the transformed human rights in the constitution is a form declaration made by the state. The protection of human rights in the rule of law, embodied in the form of norms in the regulation of laws, the next one is the enforcement through the judiciary. It is also reflected in Europe Court's Decision.

Europe Court's Decision above contains the citizens' human or fundamental rights in Schrems. Schrems's right is to protect his digital data, acknowledged in the legal cases above. It can also look like an award to the human rights or citizen rights-based European Union citizen laws poured into the *European Union Charter of Fundamental Rights*. In this European Court, the judiciary is already formed the law protection of human rights through its verdict. The enforcement by the European Judiciary in Europe also aims to ensure certainty of law, that is, that European Union law's implementation is even.

3.3 Human Rights Protection in the Shape of Arrangement Personal Digital Data Protector

Data, or in this matter, is personal digital data related to someone's human rights. People who own personal digital data can use it to identify the subject from the right or data owner (European Union Agency for Fundamental Rights and Council of Europe 2004). *The European Union Data Protection Directive (EU DP Directive), the European Union Data Protection Convention*, and *the OECD Guidelines* contain the meaning of "personal data" as all related data with people who are identified and identifiable. [11] The meaning of someone who can be identified is someone who can be known/identified directly or not directly based on ID card's numbers or based on one or other factors specific that can help in identifying physical, psychological, mental, cultural, or social.

The personal data concept above aligns with the meaning right to privacy developed by Warren and Brandeis in the journal School of Law Harvard University, "*Right to Privacy."* According to Warren and Brandeis, with the development and technological progress, a

public's awareness about the right to enjoy life will arise. [12] The journal states, "Privacy is the right to enjoy life and be left alone, and this legal development is inevitable and demands legal recognition. [13] Privacy is a right for everyone to have and enjoy life, along with the demand for privacy protection.

Privacy is one of the rights owned by each citizen. One concrete form of privacy is personal data, and of course, including in matter this is personal digital data. Data is said to be personal if the data can be used to identify somebody who owns the data. Privacy rights through personal data mean that someone can choose, determine, give, or provide or not their data.

Related to the decision court of the European Court that was explored in the study, it is seen in the case section clearly that Schrems submitted a claim or complaint to Ireland's Commission of Data Protection. The submission claim that Schrems has done happens because it is Scherms' rights to request protection of personal digital data as poured into the constitution of Ireland and the Charter of European Union Fundamental Rights.

Scherms' actions above proves that he chose not to transmit his data or provide his personal data to third countries. From case law or European Court's Decision above, it can be concluded that collecting and distributing personal data without permission violates the right to privacy. The potential of violating the right to privacy on personal data is not limited to offline and online activities. The potential appears in the activity that involves collecting personal data from someone, including on the social network Facebook. Facebook is actively collecting the personal data of the user inside his databases. The database managed by Facebook consists of the personal data of a person/user in digital form.

According to the literature, the connection of law that becomes the base rule in the case law above is the relationship of trust, sharing, and privacy. Most of the great work about trust, sharing, and online privacy focuses on how protecting privacy can increase confidence or how the perception of knowing some websites can be trusted to protect users' privacy and reduce the risk of privacy perceived by consumers. Supposedly, with such a basis, a person or Facebook media users like Scherms give their trust. In other words, maintaining user trust becomes very important for online platforms such as Facebook.

Facebook has designed a Scherms that pushes users to share each other, or as James Grimmelmann put it, to "scratch the social itch of its users. [14] " It is why the main user creates and maintains their profile in a manner public.

When people first register and create Facebook profiles, they must agree to the terms and conditions of Facebook (*Terms of Use*). Agreement or can called *permission* to agreement displayed with tick box with a link to the privacy policy. Thus, if someone wants to become a Facebook user, they must agree to the Facebook's privacy policy and terms and conditions (Terms of Use).

Even so, it does mean that Facebook users cannot resubmit the rejection to a privacy policy company as Scherms did. The objection can be submitted again because the contract (Facebook) provision does not have good etiquette or a lawful clause. [15] To show that the agreement does not fulfill the legal condition clause, the previous submission shows the abnormalities within the procedural regulator contract, such as "unequal bargaining positions, undue length, fine print, confusing language, and misleading terminology."

The terms and conditions of using Facebook are from the standard contract. However, in his research, Yasamine Hashemi [16] states that most Facebook users don't read documents thoroughly. This can support the assumptions that the contracts made by Facebook are too long and confusing or that there is no possibility that users can bargain with Facebook.

Facebook is a platform that people can use to build and deepen their connections with others. It is possible because Facebook has designed the platform in such a way as to facilitate its user's convenience to do things within its platform easily.

However, throughout these years, people or Facebook users are considered to have agreed upon the terms and conditions (*terms of use*) when they first registered as a user. In the provision, Facebook states that the users are responsible for themselves regarding the risk of using Facebook. Besides that, Facebook also allows or permits its users to arrange options regarding the limitation of access on their profile page. Facebook also states that it cannot control its users' actions, and it is the users' option to choose to share pages and use the information.

All of the common things mentioned above align with Facebook's meaning of implementing privacy rights for all users by giving them a choice to share or not share information with users other. The implication is that Facebook cannot ensure that unauthorized people will not see the shared information by its users. In other words, Facebook's privacy policy does not responsible for the equivocation of the privacy policy or any security measures on Facebook.

The only worry from Schrems as a Facebook user is to have pushed Schrems as a user for the complaint to Ireland's Commission of Data Protection. It is because it is suspected that unauthorized people can access personal data transmitted to the United States. As for the transmitted personal data by Facebook are stored and managed in the office center in the United States.

Ireland's Commission of Data Protection responds to Schrems's complaint with a refusal. The Commission assumes that the complaint does not have any legal reason basis. Ireland's Commission Data Protection states that the United States is under the safe harbor Scherms ensures the security level protection of transmitted data to the United States in Decision 2000/250.

However, the European Court decides the Commission's Decree 2000/250 is invalid. It is because Ireland's Commission of Data Protection does not state that the United States ensures sufficient protection based on domestic law or international commitment to the United States of America. The court states that Ireland's Commission of Data Protection needs to find by stating that the United States "really" ensures the level of rights protection based on domestic law or commitment to international equivalent with the guaranteed rights within European Union law.

3.4 Several Relevant Indonesian Legislation with Personal Data Protector

Specifically, regarding the protection of digital personal data in Indonesia, apart from what has been specifically mentioned above, namely what is contained in the Data Protection Law, although it does not specifically regulate the protection of personal digital data that is transmitted trans-jurisdictionally, there are still several other pieces of legislation, in this case, legislation that can be put forward as a regulation on data protection in general. For example, the arrangement related to data protection of banking arranged in the Constitution of Banking about private banks, also rights related rights privacy customers in Article 1 point (28) mentions that bank secrets are related to client deposit and savings information.

The arrangement within the constitution of banking above also enunciates the protection for its client regarding financial data (savings or other bank products), personal data characteristic client information or relevant information identity, or other personal data outside financial data. Then, to enforce personal data protection for clients, there is a regulation of criminal sanctions about the violation toward banks regulated in Article 47 Act (1) and Act (2).

Likewise, with Telecommunications Act arranged in Indonesian legislation about privacy protection, specifically owned by user service telecommunication. Article 22 of the Telecommunications Law regulates the prohibition of network and service telecommunication or telecommunication access in a manner special without right, no valid, or with manipulation. This shows personal data owned by user service transmitted telecommunications through telecommunication maintenance protected by law in Indonesia. The regulation of criminal sanctions for violating the protection privacy of personal data that used telecommunication service articles is located in Article 56 and Article 57 of the Telecommunications Law.

Indeed, in Indonesia's arrangement, the should-be-protected-by data and information by the Law of Consumer Protection are not explicitly arranged with the consumer's personal data information; instead, it is more to goods and services. The Constitution of Customer Protection only forbids offering, producing, or incorrectly advertising goods and services, as if arranged in Article 9 paragraph (1) law. However, it ruled out the possibility of the misuse potential of using consumer data emerge. Because of that, Indonesian customers do not have a solid basis of laws to ensure their privacy rights as consumers. In this matter, it still happens because there is a law vacancy of protecting consumer's personal data privacy; however, according to the Dignified Justice theory, which postulates the system, the lack within the Act of Consumer's Protection can be covered with other Constitutions that governs the data protection, including the Act of Data Protection.

The privacy right of personal data is also regulated in the Act of Human Rights. Article 32 of the Human Rights Law regulates the guarantee of independence and secrecy in connection with communication through electronic devices. Article 32 shows the balance between the right to obtain (find, obtain, store) and convey information with the right to admit its secrecy in communication, including personal data. Thus, the Constitution admits privacy rights and personal information and data protection.

The privacy right or personal data protection is also guaranteed in the Constitution of Human Rights in Article 2 and Article 8 paragraph (1) letter e. The protection of the population's data and document are emphasized in Article 79 paragraph (1) and Article 84 paragraph (1), which mention that the state needs to keep and protect personal data and the population's documents. Such prohibition of illegal access and the misuse of personal data or population documents is written in Article 77. The criminal threats toward violating privacy and additional personal data or population documents are imprisonment and regulated fines in Article 93.

The data transmission or transaction, nor the use of technology information, is closed related to ITE Law. Within the use of technology, personal data protection is one part of the privacy rights. To provide a sense of security for the users of electronic systems, the ITE Law has regulated the protection of personal data and rights contained in Article 26, paragraph (1) of the ITE Law. As determined in Article 26 Law Act ITE, using every personal information and data carried out through electronic media without its owner's permission violates privacy rights. Even so, the ITE Law does not arrange the obligation of protecting and the effort to protect, which the related parties, such as the organizer of the electronics system, supposedly do.

The protection of public data and information collected by public agencies (probably through digital platforms, is regulated in Article 6, paragraph (3) of the Act of the Information General Public's Openness. Public agencies cannot give public information related to personal rights. In addition, Article 52 of the Act of Information Public's Openness arranges criminal sanctions if a public agency purposely does not provide, give, or publish public information, such as periodical public information, mandatory public information that need to be announced immediately, public information that should be

delivered with the basis following the Constitution, and its consequence that can harm others.

Regarding protecting personal data - related to health conditions, the law is arranged in the Act of Health. The protection of a patient's medical record is located in Article 57, paragraph (1) of the Law, which recognizes the health rights of everyone and its secrecy toward the personal medical record who has consulted with the health service organizer. Meanwhile, in the Insurance and Finance Authorize Services Constitutions, the problem of protecting information by other designated parties or assigned by the Finance Authorities Service which functions as the supervisor and other regulated functions.

Besides the Constitutions mentioned above, protecting privacy on the secrecy of personal data is also regulated in Government Regulation 71 of 2019 concerning Administration Systems and Electronics Transaction. In Government Regulation, the protection of privacy in the confidentiality of personal data is arranged in several Articles, namely: Article 9 paragraph (1), Article 12 paragraph (1), Article 15, Article 22 paragraph (1), Article 38 paragraph (2), Article paragraph (1), Article 55 paragraph (3), and Article 68 paragraph (1). Then, the violation of the effort of personal data protection, the organizer's electronic systems or agent will be given an administrative penalty as there is in Article 84.

The study of several regulations of Indonesian laws related to data and the protection of data in general shows that there is an opportunity for researchers to argue that the norms used in the European Court Decision in Scherms' case have a similar meaning to the norms in Indonesian law. The norms used by judges in the decision Europe *aquo* are substantially equivalent or similar, although the formulation is different from the data protection in Indonesia law.

So, if in the future, there is a similar case to the Scherms case that happened in Indonesia, then the norm that fixes/is similar, which is found within its equivalence/similarity, can be used by the Indonesian judges or transposed to decide the problem. Thus, the concept of the rule of law according to Dignified Justice theory, which is the substance of Article 1 paragraph (3) of the 1945 Constitution, the principle of legality in Indonesia is not *vacuum* or meaning is not obscure.

4 Conclusion

At first, it seemed like there was the impression that the norm for protecting personal digital data or digital data of individual citizens, which were transmitted to Facebook users trans-jurisdictional, still contained a vacancy or *vacuum rechts*. However, with method transposition, the similar norm in the Pancasila law system can be matched or substantively after being accustomed to the law's values in Pancasila as the soul of the Indonesian people (*volkgeist*). Transposition or the study of law comparison is carried out to make reference or juridical guidelines in overcoming, clearing problems, and applying concerns regarding data protection, specifically the trans-jurisdictionally violation of the transmitted digital data privacy. Even if formulation norms differ from formulation norms applicable to personal digital data protection in the case law studied in this study, the judge can use the invention of law to form norms or the rule of law similar to the case Scherms above.

References

1. McAfee, Andrew. Erik., B.D. Mana. Rev. HBR, **90**, 60-6, 68, 128 (2012)
2. Malik, P., Governing B.D. Prin. Prac. IBM RDJ, **57**, 1-13 (2013)
3. Y. Seounmi. Det. Onl. Priv. JCA, **43** (2009)
4. Kusyanti A. Info. Priv. Con. PCS, **124** (2017)
5. T. Prasetyo. *Penelitian Hukum dalam Perspektif Keadilan Bermartabat.* (Indonesia, Bandung: Nusa Media, 2019)
6. T. Prasetyo. *Keadilan Bermartabat Perspektif Teori Hukum.* (Indonesia, Bandung: Nusa Media, 2015)
7. T. Prasetyo. Crim. Mng. Pers. Jst. Dign. JP, **XXI** (2016)
8. Adriana P. Ref. Jus. Dig. Panca. JY, **18** (2017)
9. J. Kameo, T. Prasetyo, Panca. Fir. Law. Phil. Dign. Jst. JoL ERI, **24** (2021)
10. K.S. Titon., *Interpretasi Hak-Hak Asasi Manusia oleh Mahkamah Konstitusi Republik Indonesia The Jimly Court 2003-2008* (Indonesia, Bandung: Mandar Maju 2018)
11. Mark F., E. Jason, Daniel P.C., Conv. Prtc. Indv. Respct. Auto. Prsn. Data. (1981)
12. R.E Latumahina, Aspct. Law. Prtc. Prsn. Data. in Cybrspc. JGA, **3** (2014)
13. S. Dewi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional.* (Indonesia, Jakarta: Refika Aditama, 2015)
14. James G, Svg. Fb. NYLS LSRP **94** (2009)
15. Allyson W, Onl. Priv. Pol., DLR, **111** (2007)
16. Y. Hashemi, Priv. Pol. Fb. Thrd. Prtshp. JoSTL **15** (2009)