P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

Legal Protection of HARA Platform Users on the Service of Electronic Data Interchange

Nikmah Mentari[1], Ninis Nugraheni[2], Muhammad Annas[3]

[1] *Faculty of Law, Hang Tuah University, Indonesia*
nikmah.mentari@hangtuah.ac.id
[2] *Faculty of Law, Hang Tuah University, Indonesia*
ninis.nugraheni@hangtuah.ac.id
[3] *Department of Law Universidad Carlos III de Madrid, Spain*
100433257@alumnos.uc3m.es

Abstract

Introduction to the Problem: The digital era of technology has cut the role of third parties and made it easier for services to be run peer-to-peer; where parties can connect directly at a business scale. Business relations is always accompanied by contracts. However, nowadays conventional contracts have undergone disruption with the existence of blockchain technology. A smart contract is a contract model that uses technology that can execute the contents of the contract automatically. The existence of this technological sophistication also has implications for the exchange of data, particularly personal data. Personal data can be easily accessed through the data exchange process, but it is feared that data misuse will occur. In order to prevent the Electronic Data Interchange of personal data using this technology, data must be protected.
Purpose/Objective Study: This study aims to examine the legal protection of users of the HARA platform who use smart contracts in electronic data interchange services.
Design/Methodology/Approach: This research is normative juridical research with statutory and conceptual approaches.
Findings: In this case, the protection includes preventive and repressive protection. Preventively through legislation with the presence of laws on ITE and laws on Personal Data Protection as well as internal regulation of platform providers, while repressively lawsuits can be carried out through litigation and non-litigation channels.
Paper Type: Research Article
Keywords: Legal Protection; HARA Platform; Electronic Data Interchange; Smart Contract

Introduction

Electronic data exchange (EDI or *Electronic Data Interchange* also *Electronic Document Interchange*) is a structured process of data transfer in an approved standard format, from one computer system to another, in electronic form. The term is commonly used in the context of commerce and business, particularly electronic

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

commerce or *e-Commerce* (Susetyorini, 2010). In Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) Article 1 Number 1 states that EDI is included in the unit of a set of definitions of electronic information.

Information is information, statements, ideas, and signs that contain value, meaning, and messages; both data, facts, and explanations can be seen, heard, and read presented in various packages and formats according to the development of information and communication technology electronically or non-electronically (Law Number 27 of 2022 on Personal Data Protection Article 1 number 3 (PDP Law)). Meanwhile, data is an information, especially facts or numbers, collected to be examined and considered and used to help decision-making or information in an electronic form that can be stored and used by a computer (*Cambridge Dictionary*, n.d.).

Nowadays, information and data are promising business objects. Both are the core tools used to create devices to interact with one and another. Additionally, Substance software is a more reliable resource for markets, R&D institutions, and company activities (Manzo, 2017). This opportunity then developed and became a great opportunity for start-up companies to start a new business engaged in data sharing and data exchange with blockchain technology in the context of smart contracts. Data exchange is a trend and foundational for private and public companies, given that data exchange affects the operational speed of a job, especially in business transactions. For instance, operational needsto conduct business analysis that is fast, precise and integrated, and real-time.

HARA is an interesting data exchange company to study. The HARA platform is a data exchange service provider engaged in the agricultural industry. HARA is a data-based exchange blockchain for the food and agricultural sector. A blockchain is a disintegrated ledger consisting of blocks managed by a computer network. The data is stored in such technology so when it becomes a series of blocks, it will be difficult to change the data because it has to be changed as a whole (Nugraheni et al., 2022; Putri & Mentari, 2022).

The data can be used by institutions in all sectors in order to make decisions based on this data. For example, HARA digitizes loan administration and disbursement processes of several financial institutions. In addition, data from HARA is used in market research reports to provide information on rice production in Indonesia (Hara, n.d.). HARA connects and manages data providers and buyers in an ecosystem. The types used are market-driven income distribution and ownership rating system. Data consumption and provisioning are facilitated through mobile and web applications. This application also enables data transaction integrity, acquisition, processing, storage, and analysis (White Paper, 2019).

Referring to the technology used by the HARA platform, which is in the form of *blockchain*, the framework of the agreement in the data exchange business agreement

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

is smart contract. In the use of smart contracts in the HARA platform, there are five legal relationships that occur between parties that do not involve third parties (Nugraheni et al., 2022). In these five legal relationships, each user will be attached to rights and obligations that creates a legal responsibility. This study is about the legal protection of HARA platform users as a data exchange service. Therefore, it is crucial to conduct further research on HARA platform as EDI service in contract law in Indonesia and legal protection of EDI service users on the HARA platform.

Methodology

This research is a legal normative research with conceptual and statutory approaches. The statutory approach is a research approach method that is conducted by reviewing all laws and regulations related and relevant to the legal issue being discussed (Muhammad, 2004). While the conceptual approach is a research approach which is conducted by reviewing viewpoints based on doctrines in legal studies (Muhammad, 2004). At the statutory level, it will conduct a study of the Indonesian Civil Code, ITE Law, and Personal Data Protection (PDP) Law. Meanwhile, in the aspect of the conceptual approach, the studied concept will be based on the concept of contract law and protection of the use of ITE.

Results and Discussion

Hara Platform as an Edi Service in Contract Law

Data exchange is generally interpreted as aa specific instance or case of data sharing (State of Arizona Enterprise Data Sharing, n.d.). According to the OECD, data exchange is

"the process of sending and receiving data in such a manner that the information content or meaning assigned to the data is not altered during the transmission" (OECD, n.d.). Data exchange is the transfer of large data and files between an organization and a system; while data transmission is the process of sending digital or analog data over a communication medium to one or more computing, network, communication or electronic devices. Data transmission is the process of transmitting digital or analog data through a communication medium to one or more computational, network, communication, or electronic devices (Cambridge Dictionary," n.d.) so that the information and meaning are inherent in it unaltered. Data exchange is often used to share data between business partners or suppliers in order to collaborate (Data Exchange Definition, n.d.).

The type of data consists of (Budhijanto, 2020):

1. Volunteered data. Personal data that is actively and detailed provided by individuals when registering for platform services;
2. Observed data. Behavioral data generated through observation/observation of service usage by individual users of platform services;
3. Inferred data. Data that is not active or passive is provided by individual users of platform services, but is obtained through the analysis of the data collected.

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

On the other hand, there are also the type of data exchange based on how the data exchange occurs. Some types are mentioned below (Data Exchange Definition," n.d.):

1. Data exchange *peer-to-peer*: This kind of direct exchange occurs between two organizations or two different divisions of the same organization when necessary.
2. Exchange of personal data: The data exchange is accessible by and for a specific group of users generally falls into this category. A typical example of such a breed is a group of users who share industry-specific data. Another example is when a company will share data with its suppliers who want to share it with their customers. Project-related data exchange cases can also be treated as personal data exchanges.
3. Electronic data exchange (electronic data interchange): Electronic data exchange is carried out through Cloud. The data is available to users by downloading the file. Protection addition Form Access can also be blocked with a password (*Password*).

Electronic data exchange or Electronic Data Interchange (EDI) is a new type of communication-based on direct exchanges of business data carried out electronically between computers in a standard form or standard contract. EDI allows data in the form of electronic messages to be transmitted from the place computer Edi created to another computer. After the message is entered into the keyboard of the sending computer, the message is copied to the hard disk. The computer then sends the data to the receiving computer using its communications software (Pejovic,1997). Successful data transmission electronically via satellite or telephone line where both computers are located and connected via modem (Modulator-Demodulator). The modem on the sender's side converts the digital information processed by the sending computer into an analog signal used for telecommunications over a regular network. When data is received on the receiving side, it is again converted by the modem into digital information. Received data can be stored on the recipient's computer or on the disk and retrieved when necessary, it does not need to be printed on paper. That's why EDI is often referred to as a 'paperless operation' (Pejovic, 1997).

EDI is basically an electronic transaction, a legal act regulated in Article 1 Number 2 Law Number 11 of 2008 on Electronic Information and Transactions as amended by Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law). Based on this, there are two essences of electronic transactions which include legal actions and how they occur (HS, 2020). From the aspect of legal acts, there are rights and obligations between the two parties who send and receive data. Meanwhile, from the aspect of how it occurs, it includes computers or currently can use gadgets, computer networks or internet networks and other electronic media (HS, 2020).

Article 1 Number 17 of Government Regulation Number 71 of 2019 on Implementation of Electronic Systems and Transactions an electronic contract is an agreement between the parties entered into through an Electronic System. Article 46

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

paragraph (2) states that the conditions for the validity of an electronic contract are, as follows (Rachmadani & Rosadi, 2021):

1. There is an agreement between the parties;
2. Conducted by a legal subject who is capable or authorized to represent in accordance with the provisions of laws and regulations;
3. There is a certain object;
4. The object of the transaction must not contradict the laws and regulations, decency, and public order.

In essence, EDI is Similar to data exchange contracts in general, it's just that the media used is electronic networks, computers, internet networks, or other electronic media. Regarding data exchange contracts, in the industrial era of 4.0, the media used is not just an ordinary electronic contract. However, smart contracts use blockchain technology. Smart contract is a legal product, produced from the utilization of blockchain technology which is the result of server program innovation and Decentralized computers in the revolutionary era of Industry 4.0. On the other hand, the standard contract emerged from the centralized concept of one party that has a stronger position in the standard contract. Moreover, the mechanism for issuing standard contracts in electronic contract formats, one of which utilizes a Centralized Server computer, existed long before the industrial revolution 4.0 (Serfiyani & Serfiyani, 2019).

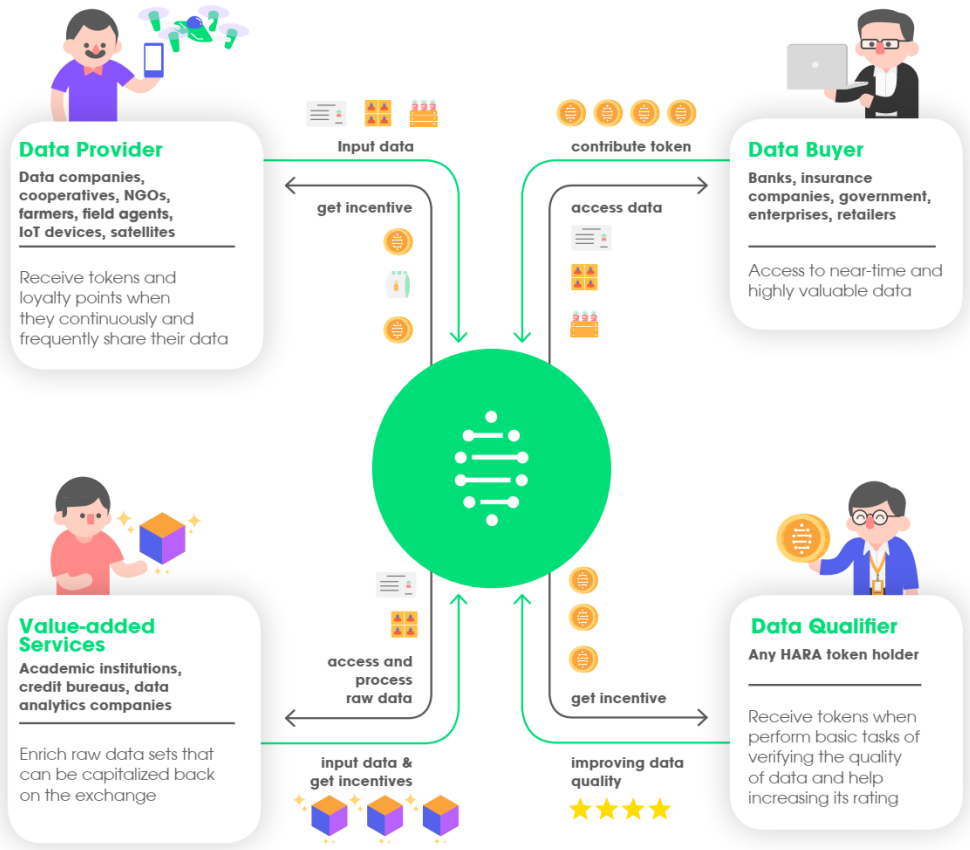
EDIs with smart contracts are found in Indonesia, one of which is the HARA platform. HARA is a data exchange provider platform engaged in agricultural industry. HARA's acquisition involves various parties such as shareholders, ranging from input suppliers, logistics, traders, and financial services to data companies (White Paper, 2019). Data that is meant as an object on the HARA platform is an agricultural-related document such as planning schedules, crop type, fertilizer, harvest schedule, and yield (White Paper, 2019). HARA leverages valuable near-time data to increase productivity, reduce losses, and create market efficiencies. In the process, the HARA team collected data from various stakeholders over the past two years. These parties consist of data providers who submit their data at HARA and data buyers who need data for decision-making processes. In addition, there is also a Data Qualifier to ensure data quality; and finally there are services that help users turn data into reference information and reports (Nugraheni et al., 2022).

Within the HARA platform four main ecosystems, along with Field Officer, they have different legal relationships in the implementation of its application, as seen in Figure 1 (White Paper, 2019).

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

JURNAL HUKUM
NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Figure 1. HARA Ecosystem and the Legal Relations of the Parties



Source : *White Paper*

1. Data Provider and HARA
   The legal relationship between the two is the Distributor Contract. Where in its implementation the data owned by farmers / providers is distributed through the HARA application, and in return the Provider will get incentives in the form of points as a medium of exchange.
2. Field Officer and HARA
   The legal relationship between the two is a Contract of Sale and Purchase of Services. In this case, the field officer will get an incentive in the form of a medium of exchange from HARA if it has helped the provider to input data.
3. Buyer and HARA Data
   The legal relationship between the two is buying and selling data. This is evidenced by the exchange of data that has been obtained from the Provider with Tokens that occurs in the HARA Application Platform.
4. Value-added Service and HARA
   The legal relationship of such activity is the Distributor Contract, which is evidenced by the legal relationship in No.1. because the subject and object on which the contract is focused are the same. In this value-added services process, it

P-ISSN: 1412-6834
E-ISSN: 2550-0090

Jurnal Hukum Novelty
Volume 14, Issue 1, 2023, pp. 51-68

is the addition of data input carried out by providers into the HARA Platform. And in exchange will get incentives in the form of points that can become a medium of exchange.

5. Data Qualifier and HARA
   The legal relationship between the two subjects is the sale and purchase of services. The qualifier is in charge of analyzing and assessing the data of the providers contained in the HARA platform. Instead, qualifiers will get incentives from HARA.

EDI on the HARA Platform is done on a global and open blockchain facilitated by smart contracts as proof of agreement of the parties. Smart contracts in Indonesia are not specifically regulated. Smart contract an innovation as it is type of electronic contract. Because of the third part of the Civil Code, smart contract may develop in Indonesia. There is potential for the emergence of new forms and types of contracts because the Civil Code which forms the basis of contract law in Indonesia is open. Smart contract is a manifestation of the parties' freedom to make a contract with the content, form, manner, and time as they agreed, which is another reason why the freedom of contract concept exists. Contractual arrangements generally refer to the provisions of Article 1320 Code Civil regarding the valid terms of the agreement, both subjectively and objectively. The enforcement of the validity of the contract gives legitimacy related to the cancellation of a contract. Moreover, if the legal conditions of the article are valid, a contract is binding on the parties, as stated in Article 1320 Civil Code.

Given that in a smart contract, the applicable properties are self-executing and *self-enforcement*; where it can automatically carry out the contents of the contract, then it will be difficult to cancel the contract since it can be canceled if the subjective conditions are not met. This is because users of the HARA platform, even though they are registered, have the qualifications as legally competent. It is possible that in the event of an EDI transaction, they act on other people who are not legally competent. Meanwhile, EDI transactions do not occur regularly face-to-face.

In addition, even though it is automatic, smart contract technology can be said to be an Electronic Agent according to Article 1 Number 8 of the ITE Law, which is a device from an electronic system that is made to take action on certain electronic information automatically. In Article 47 Government Regulation Number 80 of 2019 on Trade Through Electronic Systems (PP PMSE) also stated that an electronic contract can be made based on the results of interaction with an automated device and the validity of the electronic contract cannot be denied unless it can be proven that the automated system is not working properly. The electronic agent can be in the form of electronic data such as computer code or another form, so smart contracts in fact have no legal vacuum in application. Article 37 PP PSTE has clearly provided minimum feature limitations that must be available in its implementation, such as: features to make corrections, cancel orders, provide confirmation or reconfirmation, choose to continue or stop executing processes, view information in the form of

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Electronic Contracts or advertisements, check transaction status and read agreements before making transactions (Kadly et al., 2021).

Given the uniqueness of smart contracts with blockchain with an on-chain work system, which places identity verification and private keys in it, proficiency will definitely be fulfilled. There is a code setting that requires the recipient to provide a scan of the original identity accompanied by a selfie along with an identity card, to an electronic signature, then the recipient and user will be selected by themselves related to these skills. Refer to the objective terms of Article 1320 Code Civil and Article 46 Paragraph (2) Government Regulation Number 71 of 2019 on to Electronic System and Transaction Operation (PP PSTE) related to certain objects and *halal* causation or objects of transactions that do not violate the provisions of laws and regulations, decency or public order, broadly speaking, the purpose and objectives of a smart contract is to facilitate execution. So that the content of *smart contracts* itself (after coding) is certainly the same as conventional contracts as well as *e-contracts*, i.e. not contrary to the law (Nugraheni et al., 2022).

Therefore, the implementation of the ITE Law in Indonesia has implications for two things, which are (1) the legitimacy of transactions and electronic documents into a positive legal framework in Indonesia to ensure legal certainty; and (2) the classification of unlawful acts or criminal acts related to the misuse of information technology and electronic transactions supplemented by criminal sanctions (Rizqi & Prasetya, 2022). Based on the legal aspects of the contract contained in Code Civil, there are differences between the principles applied. In Article 3 of the ITE Law, there is a principle of benefits and a principle of prudence. Where Code Civil applied the principle of consensual and the principle of personality (*Privity of contract*) (HS, 2020).

Legal Protection of Edi Service Users on the Hara Platform

Digital technology that is utilized in the form of application platforms or through websites always intersects with data exchange. In this case, the user will enter a minimum of personal data in the form of name, date of birth, domicile, and occupation. User data that enters the system, is a guarantee to verify that the user is not a robot or in this case is indeed the legal subject of that person (natuurlijk persoon). Given the transformation of technology and information developing so rapidly, in this case, data becomes a very valuable asset. Data does not cease its usefulness as information for interchangeability (Interchange), but data as an asset that has value to trade. Data also has the potential for abuse to criminal acts in cyberspace (cybercrime).

According to Article 1 number 1 PDP Law, personal data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. Meanwhile, the classification of personal data according to Article 4 PDP Law:

1. Personal Data consists of:

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

a. Specific Personal Data; And
b. General Personal Data.

2. Personal Data that is specific in nature as referred to in paragraph (1) letter a includes:
   a. health data and information;
   b. biometric data;
   c. genetic data;
   d. crime record;
   e. child data;
   f. personal financial data; and/or
   g. other data in accordance with regulatory provisions and legislation.
3. General Personal Data as referred to in paragraph (1) letter b includes:
   a. full name;
   b. gender;
   c. citizenship;
   d. religion;
   e. marital status, and/or
   f. Personal Data combined to identify an individual.

The parties who related to personal data are Personal Data Processor and Personal Data Controller. Personal Data Processor means any person, entity the public, and international organizations acting singly or jointly in doing the processing of Personal Data on behalf of the Data Controller Personal. Moreover, Personal Data Processor means any person, entity the public, and international organizations acting singly or jointly in doing the processing of Personal Data on behalf of the Personal Data Controller (Article 1 number 5 jo number 6 of the PDP Law).

In the HARA platform, what happens is the exchange of data in the form of purchasing information (data) related to agriculture. The use of the HARA platform itself begins with information about the user's personal data, before the stage of data exchange transactions for objects in the form of agriculture. Below is a table to describe farmer's personal data collected by HARA:

Table 1. Farmer Related Data

Farmer Data	Commodity Data	Field Ownership Data	Field Data
Farmer's ID Farmer's Profile Profile Photo Selfie ID Birth Date Address	Name	Farmer Field Ownership Status Validity Status	Name Polygon Farmer's ID Farmer's Profile Profile Photo Selfie with ID Birth Date Address

Source: *White Paper*

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Based on the personal data that HARA collected, it can be concluded that the collected data is a General Personal Data according to Article 4 number 1 point b. Although Personal Data collected by HARA platform is just a General Personal Data, it cannot be denied that there is a possibility of misuse of this personal data. Particularly with the personal ID, profile photos, and Selfie ID which are also often easy to abuse. In the legal context, this data exchange business or EDI has risks to two things, namely misuse of personal data and Unlawful Acts (*Tort*). This is given that within the HARA platform, the data exchange agreement is carried out through smart contracts which use blockchain technology. Thus, there is very little default occurring. Referring to the nature of smart contracts that are self-executed and self-enforcement (Nugraheni et al., 2022). Thus, legal protection must be attached to it. The urgency of protecting data, both personal and commercial data (Rizal et al., 2019). This is because data is a new type of wealth in the Indonesian nation. Now data is more valuable than oil (*the world's most valuable resource is no longer oil, but data*-The Economist, May 2017). Therefore, data sovereignty must be realized in the form of citizens' rights to personal data that must be protected (Pidato Kenegaraan Presiden Jokowi, 2019).

Maria Theresia G. interprets legal protection as relating to state acts to do something with (enacting state law exclusively) with the purpose to provide guarantees of certainty of the rights of a person or groups of people (Mawarni, 2018). Legal protection is one of the best ways to protect a legal subject from the authority applied (Johan & Ariawan, 2021). Legal protection is broadly entrenched in terms of its legal order. Information is the primary source. In economics, and indeed for some time now, information has been regarded as an item that is very different. This is required for each transaction (e.g. Al related to every purchase on the market) and they are expensive (at least in the form of fees search and time) (Devitasari et al., 2019).

The development of information technology and communication that advances rapidly has led to various opportunities and challenges. Information technology might humans connect with each other without knowing territorial boundaries countries are one of the driving factors of globalization. Utilization of information technology results in an individual's Personal Data being very easy to collect and transferred from one party to another party without as far as Data Subject being Private, thus threatening the constitutional rights of Personal Data Subjects (General Section of PDP Law).

In the concept of information privacy and self-determination in information It can be difficult to implement when the individual does not know the things that have been given to the personal data. The concept of self-information, self-determination, It is only feasible when there is full knowledge of the number and types. The information collected and processed is available to all individuals. Without this knowledge, self-determination of information and the right to information privacy is nothing more than just a paper tiger (Devitasari et al., 2019).

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

Modern data processing technology has many advantages over other slower manual methods, but technological advances. This is certainly inseparable from some problems. One of the problems, this includes the fact that data processing may threaten individual rights over privacy. Personal data can now be combined and stored without the existence of limitations and it is also very accessible than in the era before the progress of this technology. Personal data may be disseminated and manipulated information in each field and often without the knowledge of the data owner. Much less It is possible that governments and business enterprises are collecting information from citizens that poses a potential threat to individual freedom (Devitasari et al., 2019).

Personal Data stored in Electronic Systems shall be Data Personal whose accuracy has been verified. Personal Data stored in Electronic Systems must be in the form of encrypted data. Personal Data is required stored in the Electronic System in accordance with the provisions of laws and regulations-An invitation that regulates retention term obligations of Personal Data at each of the Supervisory and Regulatory Agencies of the Sector (Devitasari et al., 2019). Currently based on Law Number 27 of 2022 on Personal Data Protection (PDP Law), Article 21 Paragraph (1) letter d, the Personal Data Controller is obliged to submit information related to the retention period of the document containing the Personal Data, letter f the period of processing the Personal Data. Explanation on letter f i.e. the means "the period of processing the Data Personal" is the time span from start to completion of a series of Data processing activities Personal according to the purpose processing of Personal Data. Article 32 paragraph (1) The Personal Data Controller shall provide access to Personal Data Subjects to Personal Data processed along with the track record of data processing Personal according to the term Storage time Personal Data. In this case, the PDP Law does not affirm the time period in a rigid manner, it shows the flexibility of the PDP Law to each electronic system operator.

Protection of Personal Data is included in the protection of human rights Thus, the regulation regarding Personal Data is a manifestation of the recognition and protection of basic human rights. PDP Law Order of Article 28G paragraph (1) of the Constitution of the Republic of Indonesia of 1945 which stated that "Everyone has the right to self-protection person, family, honor, dignity, and property under his power, as well as the right to a sense of security and protection from threats Fear of doing or not doing a session that is a right ". Personal Data Protection issues arise because of concerns about Personal Data that may be experienced by people and/or legal entities. That these violations can cause material and non-material losses (General Section of the PDP Law).

The reasons privacy should be protected are: First, in cultivating relationships with others, a person must cover part of his personal life so that Data Owner can maintain his position at a certain level. Second, a person in his life needs time to be alone (Solitude) so privacy is indispensable for someone. Third, privacy is a stand-alone

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

right and does not depend on other rights, but this right will be lost if the person publishes private matters to the public (Rosadi, 2017). Fourth, privacy also includes a person's right to domestic relations including how a person fosters marriage and fosters his family, and others should not know about those personal relationships so then Warren referred to it as 'the right against the word'. Fifth, another reason why privacy deserves legal protection is that the losses suffered are difficult to assess. The loss is felt much greater than the physical loss because it has interfered with his personal life so if there is a loss suffered, the victim must get compensation (Rosadi, 2017). The concept of personal data protection emphasizes that everyone has the right to determine their own destiny as to whether they would do data sharing or not. If data sharing is conducted, then they have the right to also determine the conditions to be met in a community (Priscyllia, 2019).

Legal protection is divided into two; namely, preventive legal protection and repressive legal protection. In preventive legal protection, the people are given the opportunity to raise objections (inspraak) or their opinion before a government decision gets a definitive form. Thus, Preventive legal protection aims to prevent disputes from occurring while on contrary repressive legal protection aims to resolve disputes (Musfianawati, 2014).

Based on the preventive aspects of EDI services for HARA platform users, it is at the regulatory and internal mitigation levels. Currently, regulations related to electronic transactions and EDI have been accommodated through the ITE Law and the PDP Law. Article 26 Paragraph (1) of the ITE Law states that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. So that if the right is violated, Paragraph (2) gives the right for the data owner to file a lawsuit for the loss. Furthermore, Paragraph (3) requires each operator of an electronic system to delete irrelevant electronic information and/or electronic documents that are under its control at the request of the person concerned based on a court determination. In addition, Paragraph (5) obliged the operator of the electronic system to provide a mechanism for the deletion of electronic information and/or electronic documents that are no longer relevant. In this case, the HARA platform as the operator of the electronic system must fulfill the mandate of the ITE Law related to personal data protection.

Specific data protection for handling EDI transactions is currently accommodated through the recently passed PDP Law. The HARA Platform occupies the positions of Personal Data Controller and Personal Data Controller. Article 9 of the PDP Law stated that Personal Data Subjects are individuals to whom Personal Data is attached (Article 1 Number 6 of the PDP Law) has the right to withdraw the approval for the processing of Personal Data about them that has been given to the Data Controlling Person. Article 10 of the PDP Law stated that the person has the right to object to decision-making actions solely based on automatic processing, including profiling, which creates a legal consequences or impacts indicating rights to Personal Data Subjects.

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

In this case, the user has the right to cancel the data exchange processing and even object to the Self-executing action. Article 65 CHAPTER XIII on the Prohibition of the Use of Personal Data of the PDP Law states that:

1. Everyone is unlawfully prohibited from obtaining or collecting Personal Data that is not his with the intent to benefit oneself or others who can result in the loss of the Personal Data Subject.
2. Everyone is unlawfully prohibited from disclosing Personal Data that does not belong to him.
3. Any Person is prohibited from unlawfully using Personal Data that does not belong to him,

With regard to preventive legal protection from the internal aspect of mitigation, the HARA platform has standards for fulfilling obligations that must be carried out by users, in the form of (White Paper, 2019):

1. Assent
   Data providers agree to consent to the storage of personal data in an encrypted format. They can decide whether or not they allow data buyers to access their data. In the HARA data exchange platform, document encryption is realized through the use of algorithms AES-256 in generating encryption keys. The encryption key is further broken down into several A keys known as a secret key. Secret keys are distributed among provider wallets data, HARA systems, and trusted third parties (eg. Government, value-added service providers). To decrypt data, a minimum of three keys are required. Any party (other than the data provider) those with a key cannot decrypt data without the consent of the other key holders.
2. Purpose Limitations
   The data buyer must inform the data provider of the intended use of the data set, which will be stated and mutually agreed upon in the purchase agreement.
3. Ad
   Data providers are notified whenever a data buyer wants to access their data. This is realized through a smart contract document provider which grants access permission to the stored data. When a data buyer wants to access data, the system notifies the data owner or data provider through the blockchain. Blockchain verifies data availability using evidence of the existing smart contracts.
4. Access and Correction
   The data provider has full ownership of its data set. They have access and full control to create, edit, and modify data. HARA only provides access information in this ecosystem.
5. Accuracy
   Every effort is made to ensure accurate personal data is collected. For example: in the case of farmers as data providers, field officers are assigned to assist farmers in verifying, uploading, and maintaining data in the HARA application. In addition, HARA's data exchange platform provides a data qualification mechanism that

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Powered by the Data Rating feature to evaluate data sets based on inputs such as historical transactions, and buyer feedback and connected data points.

6. Protection
   Data is stored securely and processed on HARA's data exchange platform. A combination of Web permanent IPFS, Blezelle protocol and Amazon web services (S3 and Dynamo DB) will be implemented as a data storage system of the chain. Proof of existence *smart contract* issued in the blockchain to ensure data is not easy broken and did not compromise. Each data is signed with evidence such as fingerprints. If The data is changed, then the associated fingerprint will also change. To verify data, fingerprints must be appropriate or considered tampered with. Nevertheless, data providers must also ensure that secure and reliable data storage and accessible mechanisms remain awake
7. Storage
   Data providers have full control when data is made accessible and can set a period to allow data access.
8. Infringement Notification
   The designated data protection officer will notify the supervisory authority and shareholders (*Data providers, data buyers, and value-added service providers*) of any high-priority and undue data breaches.
9. Data Deletion
   HARA's data exchange supports the right to rectification and erasure. Absolute data providers control their data sets. When an account is deleted on the platform, the private key will be destroyed, implying the loss of appropriate and encrypted data.
10. Privacy by Design
    The platform architecture ensures:
    a. The data provider owns the personal data and has full control over it.
    b. Personal data is always encrypted and the data provider holds the key to decrypt it.
    c. Transactions of personal data within the ecosystem are carried out with the explicit permission and consent of data providers. Data providers also understand how data sets are used and for what purpose.
    d. Personal data transactions are fully transparent and traceable on the blockchain and the anonymity of the trading parties is strictly protected.

The services and provisions provided by the HARA platform in order to mitigate the risk of data misuse is in accordance with the mandate of the ITE Law and the PDP Law based on the fulfillment of the obligations of consent, protection, storage, and deletion of data, both personal data and data related to ownership by the data provider as a user.

Based on the protection of repressive law, civil lawsuits can be filed both through litigation and non-litigation channels. In the event of a civil suit, an electronic system operator can be said to have committed an unlawful act or tort if an action of the

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

operator causes harm to the owners of good personal data due to negligence or intentionally causing the leakage of such data so that publicly accessible. Such data leaks can cause organizers may be held legally liable as a result of data leakage laws then, the organizer can be challenged on the basis of error in accordance with provisions of Article 1365 Civil Code or on the basis of impropriety or inappropriateness prudence as set forth in Article 1366 Civil Code (Baiq, 2021).

Article 26 paragraph (2) of the ITE Law 2016 clearly states that any person has the right to file a lawsuit for damages incurred under the Act. It should be interpreted that what is meant by rights here is (Rachmadani & Rosadi, 2021):

a. Personal rights are the right to enjoy private life and be free from all kinds of interference.
b. Personal rights are the right to be able to communicate with others without spying.
c. A personal right is the right to monitor access to information about a person's personal life and data.

Thus, if there is a data leakage and the sale of personal data carried out by the parties either intentionally or due to negligence, it is a civil violation regulated in Article 38 and Article 39 of the ITE Law which states that everyone can file a lawsuit against other parties that cause losses. Civil lawsuits or other dispute resolutions such as arbitration, or other alternative dispute resolution institutions can be carried out in accordance with the provisions of the laws and regulations. Relating to cross-Country transactions, Article 18 of the ITE Law states that electronic transactions are embedded into electronic contracts with the freedom to determine the law that applies to international electronic transactions. The parties are also given the ability to establish a court forum, arbitration, or dispute resolution institution that may arise from international Electronic Transactions made by them.

Meanwhile, in Article 64 paragraph (1) PDP Act Dispute resolution of Personal Data is conducted through arbitration, courts, or institutions other alternative dispute resolution in accordance with provisions of laws and regulations. Paragraph (2) of Article 64 of the PDP Law does not distinguish the procedural law in general with the procedural law that will be applied to personal data disputes unless otherwise stipulated in the law. The privileges of the PDP Law which highly uphold privacy are in accordance with the principle of confidentiality contained in Article 3 point h of the PDP Law. This seems to expressly provide an opportunity if deemed necessary, for the resolution of dispute can be resolved behind closed doors (Article 64 Paragraph (4) of the PDP Law)

If what stands out in ITE Law is the principle of neutral technology, then in this PDP Law there are two interesting principles, namely the principle of balance and the principle of accountability. The explanation of Article 3 of the PDP Law is related to the principle of balance, namely Personal Data Protection efforts to strike a balance

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

P-ISSN: 1412-6834
E-ISSN: 2550-0090

between the right to Personal Data on one side with the right of a legitimate state based on the public interest. Although personal data is part of human rights and part of private law, it does not rule out the existence of the State to take part in the protection of such privacy rights.

Meanwhile, the explanation of the principle of responsibility is that all parties related to the processing and supervision of Personal Data act responsibly so as to be able to guarantee the balance of rights and obligations of the parties concerned, including the Personal Data Subject. That is, there is an inherent liability related to personal data when the operator of the electronic system runs the business in the field of data exchange in particular. In fact, responsibility for such personal data is also attached to the data owner or the personal data subject. In this case, it is necessary to understand that personal data would not exist without the role of the party providing the data or the subject of the personal data. Hence, it is appropriate if the data owner themselves must also be responsible for the validity of the data provided to the operator of the electronic system.

Conclusion

That the HARA Platform as an EDI Service in Contract Law is within the scope of contract law contained in the Civil Code and the ITE Law. The type of Personal Data collected by HARA is General Personal Data. As the internal aspect of mitigation, the HARA platform has standards for fulfilling obligations that must be carried out by users. In addition, with regard to the Legal Protection of EDI Service is implemented through preventive protection and repressive protection. In preventive protection, namely the existence of legislation through the Code Civil, the ITE Law, and the Personal Data Protection Law. Meanwhile, repressive protection can be carried out through litigation and non-litigation. Both protections are included in the laws and regulations in Indonesia.

Acknowledgment

This research is funded by the Research and Community Service Institution (Lembaga Penelitian dan Pengabdian Masyarakat/LPPM) University of Hang Tuah Surabaya Fiscal Year of 2021

Declarations

Author contribution	:	Author 1: initiated the research ideas, instrument construction, data collection, analysis, and draft writing; Author 2: revised the research ideas, literature review, data presentation and analysis, analysis, and draft writing, and the final draft; Author 3: data presentation and analysis, analysis, and draft writing.
Funding statement	:	This research is funded under Research Project Fiscal Year of 2021.
Conflict of interest	:	The authors declare there is no conflict of interest.

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 14, Issue 1, 2023, pp. 51-68

Additional information : No additional information is available for this paper.

References

Baiq, P. A. (2021). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif. *Diktum: Jurnal Syariah Dan Hukum*, *19*(2), 149–165. https://doi.org/10.35905/diktum.v19i2.2463

Budhijanto, D. (2020, September 26). *Virtual Jurisdiction: Indonesian Digital Economy in Covid-19 Pandemic: Virtual Conference on Law*. Virtual Conference on Law, Legalaccess.id.

Cambridge Dictionary. (n.d.). Retrieved April 2, 2023, from https://dictionary.cambridge.org/dictionary/english/data

Data Exchange Definition. (n.d.). *G2*. Retrieved October 3, 2022, from https://www.g2.com/glossary/data-exchange-definition

Data Transmission. (n.d.). *Collins Dictionary*. Retrieved October 3, 2022, from https://www.collinsdictionary.com/dictionary/english/data-transmission

Devitasari, A. A., Anindyajati, T., & Ghoffar, A. (2019). *Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital* (pp. 1–99). Pusat Penelitian dan Pengkajian Perkara, dan Pengelolaan Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi. https://www.mkri.id/public/content/infoumum/penelitian/pdf/hasilpenelitian_123_Penelitian%20Hak%20Privasi%20dan%20Studi%20Komparasi.pdf

Hara (n.d.). *About Us*. Retrieved September 22, 2022, from https://www.hara.ag/about-us

HS, S. (2020). *Electronic Contract Law*. Depok: Rajagrafindo.

Johan, S., & Ariawan, A. (2021). Consumer protection in financial institutions. *Legality : Jurnal Ilmiah Hukum, 29*(2), 173–183. https://doi.org/10.22219/ljih.v29i2.16382

Kadly, E. I., Rosadi, S. D., & Gultom, E. (2021). Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura. *Jurnal Sains Sosio Humaniora*, *5*(1), 199–212. https://doi.org/10.22437/jssh.v5i1.14128

Manzo, V. (2017). The Internet of Things and Intellectual Property Rights: The Protection of Data. University of Turin -Law School, *WIPO Academy* .1–14.

Mawarni, R. (2018). Perlindungan Hukum Bagi Para Pihak Dalam Transaksi E-Commerce Melalui Facebook Progresif*: Jurnal Hukum*, *10*(1). https://doi.org/10.33019/progresif.v10i1.180

Musfianawati. (2014). Perlindungan Hukum pada Pemenuhan Hak Anak atas Akta Kelahiran. *Jurnal Rechtens*, *3*(1), 108–119. https://doi.org/10.36835/rechtens.v3i1.95

Muhammad, A. (2004). Hukum dan Penelitian Hukum. Bandung: PT Citra Aditya Bakti.

Nugraheni, N., Mentari, N., & Shafira, B. (2022). The Study of Smart Contract in the Hara Platform under the Law of Contract in Indonesia. *Scholars International Journal of Law, Crime and Justice*, *5*(7), 273–285. https://doi.org/10.36348/sijlcj.2022.v05i07.005

OECD. (n.d.). *Glossary*. Retrieved October 3, 2022, from https://stats.oecd.org/glossary/detail.asp?ID=1355

Article History
Submitted 3 January 2023 - Revision Required 17 April 2023 - Accepted 30 April 2023

Volume 14, Issue 1, 2023, pp. 51-68
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Pejovic, C. (1997). Legal Challenges In The Implementation Of Electronic Data Interchange In Transport Documents. *PPP God*, *39*, 13–36.

Pidato Kenegaraan Presiden Jokowi. (2019). *Kompas*. https://jeo.kompas.com/naskah-lengkap-pidato-kenegaraan-2019-presiden-jokowi.

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi dalam Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3). https://doi.org/10.29303/jatiswara.v34i3.218

Putri, U. T., & Mentari, N. (2022). The Future of Blockchain Technology for Sharia Banking in Indonesia. *Hang Tuah Law Journal*, 1–19. https://doi.org/10.30649/htlj.v6i1.68

Rachmadani, F. A. S., & Rosadi, S. D. (2021). Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada Smart Contract Ditinjau Dari Hukum Positif Di Indonesia. *Jurnal Sains Sosio Humaniora*, *5*(1), 650–664. https://doi.org/10.22437/jssh.v5i1.14838

Rizal, M. S., Yuliati, & Hamidah, S. (2019). Perlindungan Hukum Atas Data Pribadi Bagi Konsumen Dalam Klausula Eksonerasi Transportasi Online. *Legality : Jurnal Ilmiah Hukum*, *27*(1), 68–82.

Rizqi, L. A. M., & Prasetya, D. F. (2022). Urgensi Penggunaan Smart Contract dalam Transaksi Jual Beli di E-Commerce. *Jurnal Hukum Lex Generalis*, *3*(4), 327–338. https://doi.org/10.56370/jhlg.v3i4.247

Rosadi, S. D. (2017). Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Dikaitkan Dengan Undang-Undang No 11 Tahun 2008 Tentang Ite Dan Peraturan Bank Indonesia No 7/6/PBI/2005. *Sosiohumaniora*, *19*(3). https://doi.org/10.24198/sosiohumaniora.v19i3.11380

Serfiyani, C. Y., & Serfiyani, C. R. (2019). Kajian Hukum Teknologi Blockchain dan Kontrak Pintar di Industri Jasa Keuangan. *Buletin Hukum Kebanksentralan*, *16*(1), 39–60.

State of Arizona Enterprise Data Sharing. (n.d.). Memorandum of Understanding. *Definition*. Retrieved November 25, 2022, from https://aset.az.gov/sites/default/files/Arizona%20Interagency%20Data%20Sharing%20Memorandum%20of%20Understanding%20v2-1.pdf

Susetyorini, P. (2010). Pelaksanaan Sistem Elektronic Data Interchange (EDI) di Pelabuhan Tanjung Emas sebagai Alternatif Prosedur Kepabeanan. *Pandecta*, *5*(2), 132–140. https://doi.org/10.15294/pandecta.v5i2.2297

White Paper. (2019, M March). Retrieved from HARA: https://www.hara.ag/