

# REGULATING DIGITAL DATA PRIVACY IN INDONESIA (A DIGNIFIED JUSTICE PERSPECTIVE)

**Jeferson Kameo, Satya Wacana Christian University**  
**Teguh Prasetyo, Pelita Harapan University**  
**Rizky PP Karo Karo, Pelita Harapan University**

## ABSTRACT

*Regulating digital data privacy has become a concern in the Indonesian Legal System or the Pancasila Legal System. It is particularly important with regards to the data privacy in the block-chain technology. The block-chain technology has brought about positive development for businesses in Indonesia, but it also has negative impacts. Simultaneously, some said that there is no law governing this technology in the Indonesian System to control, particularly the aspects related to the data privacy. Therefore it appears that apart from the positive impacts of block-chain to improve the efficiency of time and transactions cost, on the other hand, block-chain gives opportunity to the beginning of cybercrime, i.e. data theft of the client's financial data. This legal research has been conducted to examine norms, the laws and regulation on data privacy protection. It has been found that the accusation of many that there is no law governing the protection of the digital data, particularly aspects of block chain is not true. It has been found in examining the aspects of legal protection in the Indonesian Legal System that there is enough existing laws and delegated legislation provided for parties involve on the usage of block-chain to protect the transactions, particularly protecting the digital data privacy within the law.*

**Keywords:** Data Privacy, Regulation, Pancasila, Dignified Justice

## INTRODUCTION

The development of technology in Indonesia has been increasing very fast. The country has declared herself as entering the industrial revolution 4.0 and ready to embrace the industrial revolution era/society 5.0. In terms to the legal system, the Indonesian Government has anticipated the newly industrial development in order to protect its citizens and people who uses technology to support their daily needs. One indicator of it is that the Indonesian Legislator and Government has formed Law No.11 of 2008 on the Information and Electronic Transaction. This Act has been amended by Law No.19 of 2016 (ITE Law).

In this paper, one aspect of law to be examined is the existing Indonesian regulation that has been formed to control the block-chain technology system. As it has been acknowledged that the use of bitcoin as the virtual currency has reached a very high pecuniary value. Block-chain is a simple digital data structure that cannot be modified. Every single data inside a block-chain is inter-connected. Therefore if there is a change in one data block, it will affect the rest of the data on another blocks. The legal problem is that bitcoin transactions are done anonymously or without disclosing the identity of the parties to the transaction. There is no need to submit many kinds of information usually requested by bank. Ssuch as source of funding, the purpose of the transaction and the address of the receiver. Due to the absence of authority that oversees bitcoin,

questions arising as to the origin of the fund itself, and for which the transaction it was conducted.

Another problem is that Bank Indonesia has stated that virtual currency has no underlying guarantees for this electronic transaction. Therefore it could cause a potentially instability in the financial system. As bitcoin in principle is regarded as crypto currency, Bank Indonesia has risen a concern that this technology could be manipulated for money laundering crime. In fact, the law No. 8 Year 2010 (TPPU) was made to regulate the prevention and eradication of the Money Laundering crime. It was made to prevent and eradicate the instability of the economy and the integrity of the Indonesian financial system. The Act also made to mitigate pecuniary harms created to life of the community, nation, and State as a result of transactions related to enormous amount of money. From the idea of law as postulated by the Indonesian Jurisprudence i.e. the Dignified Justice Jurisprudence, the Act is based on Pancasila the highest law above the Constitution of the Republic of Indonesia 1945.

It has also established in the Act an Indonesian Reporting Centre and Financial Transaction Analysis (PPATK). This State Agency is an independent body. One of the PPATK's tasks as stated in section 44 subsection (1) Letters (f) of the TPPU Law is to recommend to law enforcement agencies sensitive data obtained from tapping or having the power of interception on the electronic information and/or electronic documents. This power could also be used in order to control the block-chain system.

## RESEARCH METHODOLOGY

The method used in this research is the *sui generis* method in legal research, called normative legal method. The normative studies is a process of finding principles or doctrines of law to address and resolve the issues at hand (Prasetyo, 2019).

The normative methodology is primarily using law materials consisting of regulations, and in this research laws and regulations on banking-related electronic information and transaction. The analysis used in this research is descriptive qualitative. It processed legal materials obtained through reading of legal documentation retrieved. Data analysis is qualitative.

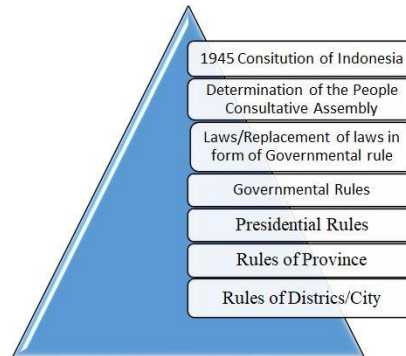
### A Brief on the Dignified Justice Theory

Dignified Justice is a newly Indonesian Grand Legal Theory. It serves to explain and give justification, particularly on the Indonesian system of law, which is different to the dominant legal theories. It explains and gives justification to a system of law by postulating among others that the law exist and grow in the nation's spirit or *Volksgeist*. For Indonesia the Spirit is Pancasila as the Indonesian People First Promise (Contract). Pancasila is the source of all sources of Law; it is the Indonesian highest Law that inspires and gives lives to every single and existing regulations in the Pancasila Legal System (Prasetyo, 2015; Rizky, 2019).

In the perspective of the Theory of Dignified Justice, or Dignified Justice; justice is where the three purposes of law and regulation as expressed by Gustav Radbruch (fairness, certainty and benefit) are united in the Dignified Justice. The Justice is exist to pursue the human dignity within every civilized social context.

From the Dignified Justice Philosophy or Jurisprudence point of view, Dictated by the *Pancasila* the Law No. 12 of 2011 regarding Formation of Legislation (Law 12/2011) is an umbrella law for the competent authority to make any necessary regulation. One of the writer of this article (Prasetyo, 2019), has argued in line with the principle enshrined in the Indonesian Constitution, the Rule of Law; that a good regulation is a regulation that has a clarity of purpose, clarity of the language, and it is not contrary to other regulations in creating the meaning of harmony and is applicable to all society.

Under the law 12/2011, with some amendments in 2019, the material of legislation must reflect the principles as follows: a) The protection; b) Humanity; c) Nationality; d) Family values; e) Values of Nusantara; f) Bhinneka Tunggal Ika (Unity in Diversity); g) Justice; h) equality before the law and government; i) order and legal certainty; and/or j) balance, harmony, and alignment. Under article 7 paragraphs (1) of the Law 12/2011, the type and the hierarchy of legislation consists of the following in the form of a pyramid.



**FIGURE 1**

### **KARO-KARO'S HIERARCHY OF LEGISLATION IN THE PANCASILA LEGAL SYSTEM**

Apart from the hierarchy of legislation stipulated in the Article 7 paragraph (1) of the Law of 12/2011, there are statutory instruments established by the delegated authority. All the delegated legislation are also recognized regulation and all are binding. The mandate is set forth in the Article 8 paragraph (1) and paragraph (2) of the Law. Article 8 paragraph (2) of Law 12/2011 contained the following formulation: "type of Legislation other than, as referred to in article 7 paragraph (1) covers the rules set by the People Consultative Assembly, the House of Representatives, the Regional Representative Council, Supreme Court, Constitutional Court, the Judicial Commission, Financial Examiners, Bank Indonesia, Ministers, body, agency, or Commission level established by law or The Government at the behest of the Act, the House of representatives, Governor of the Provinces, Representatives of regional district/city, regent/mayor, head of a village."

Article 8 paragraph (2) of the Act 12/2011 has also contained a stipulation that: "Legislation as referred to in paragraph (1) recognized its existence and had force of law that binds to all instructed by higher Legislation or established based on authority."

Delegated Legislation such the Ministerial Regulation, Regulation of the authorized Authority, such as the regulation of the Financial Services Authority (OJK), Indonesian Central Bank Regulations governing the utilization of information technology such as block-chain technology are also the existing law in the Indonesian Volksgeist.

All such a laws governing and affect the stability of the payment system and the stability of the financial system. All of these regulation are supported by the sanctions mentioned in the Acts where those provisions are derived. It is stipulated in the Article 15 paragraph (1) of the Law 12/2011 that the material provisions concerning the criminal charge can only be loaded in: a. law; b. applicable local province laws; or; c. applicable local district/city rules. All of these laws have been used to promote reforms in the Pancasila Legal System, including in this are laws pertaining to the use of Information Technology and Telecommunication, (Prasetyo, 2017) not least of them are provisions regulating the blockchain technology and in particular the protection on the data privacy.

## Legal Dimensions on the Digital Data Privacy

Regulation containing legal dimensions governing digital data privacy could be found in the Government Regulation No.82 of 2012 on the Organization of the Electronic System and Transaction (PP 82/2012). This legislation is the legal basis of a business actors both private or Government on Electronic System and Transaction, either online or off-line (Hukum,2017).

It is stated as definition of the Organizers of Electronic Systems (Penyelenggara Sistem Elektronik) according to article 1 (6) of the Information Technology and Electronic Transaction Act that: “everyone, organizers of the State, community, and business entities that provide, manage and/or operate electronic systems, both individually or together to the user electronic systems for the purposes of self-and/or needs of others.” Whereas meaning of the utilization of electronic systems provided in the Act is “utilization of an electronic system by the organizers of the State, people, business entities, and/or the community.”

The Government Regulation No. 82 of 2012 firmly set the mandatory obligation for the Organizers of Electronic System the need to guarantee: a) The availability service level agreements (Art. 12 Paragraph 1a); b) Availability of secure information agreement on the information technology services used (Art. 12 Paragraph 1b); and c) Information security and means of internal communication is organized (Art. 13 Paragraph 1c); d) Compulsory to apply risk management against damage or loss (Art. 13); e) Keeping all personal data managed classified, intact, and available (Art. 15); f) Ensure that the acquisition, deployment, and utilization of Personal Data is based on the consent of the Personal Data owner, unless it is regulated otherwise by the laws and regulations (Art. 15); and g) Ensure the use or disclosure of the data is done based on the consent of the Personal Data owner and in accordance with the purposes for which it was delivered to the Personal data owner on data acquisition time (Art. 15) (Siahaan, 2005).

It has also been regulated in POJK No.13 the year 2018 that the organizer is obligated to carry out the principle of self-monitoring (self-assessment). The principle must include: a) Principles of corporate governance of information and communication technologies in accordance with regulation of legislation; b) Consumer protection in accordance with the rules of the financial services authority; c) Education and socialization to consumers; d) Confidentiality of data and/or consumers information including data and/or transaction information; e) Principles of risk management and prudence; f) The principle anti-money laundering and terrorism funding prevention in accordance with the provisions of the legislation; and g) Inclusive and the principle of information transparency. The monitoring and evaluation are reported periodically to OJK.

The organizers formed the Association of organizers in order to have a consistent operational standard and to monitor the financial risk (Hukum, 2018).

The organizer is obligated to draw up policies, procedures for the following aspects: a) The business strategy; b) Consumer protection; c) Risks and capital; d) Human resources development; e) Development and product planning and services; f) Information technology operations; g) Communication network; h) security of information; i) Disaster recovery plan; j) User services; k) Utilization of information technology service provider; the organizer is obligated to put a data center and disaster recovery center in the region of Indonesia (Hukum, 2018).

All of the laws as stated above have also been supported by Law No.8 of 1999 on Consumers Protection (Law 8/1999). It has been clearly stated in this Law that business actors have the right to: a) Receive payment in accordance with the agreement on the conditions and the exchange rate of the goods and/or services traded; b) Right of legal protection from the consumers with no good will; c) The right of self-defense in the judicial settlement of consumer disputes; d) The right to rehabilitation of honor when it is legally proved that the consumers loss

was not caused by the goods and/or services listed; e) The rights set forth in other provisions or legislation.

The act of Information Technology and Electronic Transaction has also mandated that technological transaction is implemented with purpose to: a) Improve the life of the nation in the matter of information; b) Developing the national economy in order to improve the welfare of society; c) Increase effectiveness and public service efficiency; d) Provide a massive opportunity to every human being to advance their way of thinking and their ability in the utilization of information technology as efficient as possible and responsibly e. provides safe, justice, and legal certainty for both users and actors of the information technology.

The protection of data privacy when utilizing block-chain could also be based on agreement. This is also recognized in the Article 1320 of the Indonesian Civil Code (KUHPerdata). With agreement between the parties to every contracts, including contract using the Information Technology and Telecommunications, the security on the data privacy could also be achieved.

The Government strongly declares that bitcoin, as a virtual currency cannot be used as means of payment. Based on Law No. 7 of 2011 on Currency (Law 7/2011) jo. Bank Indonesia regulation (PBI/Peraturan Bank Indonesia) 18/40/PBI/2016 on Conducting of Payment Transaction Process jo. PBI 19/12/PBI/2017 on Financial Technology Conducting stated that payment transactions and finance in Indonesia is obliged to use the Rupiah.

The Central Bank of Indonesia has not regulated block-chain as a method of payment. In that the Bank has issued Indonesian Bank Regulations 18/40/PBI/2016 on Conducting of Payment Transaction Process (PBI 18/2016) and Indonesian Bank Regulation 19/12/PBI/2017 on Financial Technology Conducting (PBI 19/2017).

According to PBI 19/2017 classifies block-chain as a financial technology conductor or as a category in a payment system. The payment system includes authorization, clearing, final settlement, and execution of payment. By referring to its function written above, block-chain doesn't need a third party as a medium, if the system is not being controlled than it could be a media of money laundering.

Bank Indonesia must select strictly the block-chain business authors in the banking sector, specifically oversaw whether the submission of block-chain business is in accordance with the principles of belief, principles of discretion and know your customer (KYC) principle. If it has fulfilled all four principles then the perpetrator of block-chain is eligible of business permission.

Based on all the laws existing in the Pancasila Legal System as mentioned above, it could be argued here that including in the protection for the digital data privacy, for example block-chain system are regulations that could guaranty the increase customers confidence.

The Law as mentioned above, have many advantages including: Security against transaction data that is reasonably safe and can be used to record transaction data in many interrelated blocks, it's safe and not only functional in terms of virtual currency but also up to voting in an election. The laws are also support the expectation within the principle of trust and transparency.

In reality, consumers are in a very weak position, consumers adopting the block-chain system are helpless in the matter of loss. Therefore the financial activities must also be follow by a strong consistency as stated in the Financial Services Authority (OJK) No.13/POJK.02/2018 (2018 Year RI State Gazette, No.135, State Gazette Supplementary No.6238) about Financial Innovation in Digital Financial Services Sectors.

POJK 13/2018 os obliged the author of Digital Finance Innovation (IKD/Inovasi Keuangan Digital) to apply basic principles of consumer protection as already mentioned previously in the Article: a) Transparency, b) Fair treatment c) Reliability, d) Confidentiality & security of consumers data/information, e) Complaint handling and dispute settlement to be done

simply, fast, and with an affordable price, f) Provides technology-based consumer service center. OJK also authorized to perform certain actions (Art. 40 POJK).

Based on 13/2018 POJK Article 1, Digital Financial Innovation (IKD) is an activity of the renewal of business processes, business model, and the financial instruments that provide new value added in financial services sectors by involving the digital ecosystem. OJK as authorized State institutions on the financial services sector have the authority conducting the testing mechanisms for assessing the reliability of business processes, business models, finance & governance instrument Organizer who organizes the IKD, the authority is known as “regulatory sandbox”.

Based on Article 4 POJK 13/2018, OJK give criteria in doing IKD: a) Are innovative and future oriented; b) Use of information and communication technology as a primary means of administering services to consumers in the financial services sector; c) Support the financial literacy and inclusion; d) Beneficial and can be used widely; e) Can be integrated in existing financial services; f) Using a collaborative approach; and; g) Take notice of aspects in consumer protection and data protection. This mandatory IKD criterion must fulfill the requirements of the regulatory sandbox.

Based on this, a 13/2018 OJK POJK require organizer to perform three (3) a legal obligation, namely: 1. The application for registration. This obligation is excluded for the parties that have been registered or have received permission from OJK. As for the required documents is a) A copy of the organizer’s legal entity deed of incorporation along with the identity of the completeness of the data administrators; b) A brief explanation in writing of the product; c) Data and other information related to the activities of the IKD; and d) A business plan.

Organizer must also perform 2. Meet Regulatory Sandbox. OJK establish organizers to be tested in Regulatory Sandbox. This assignment is done against the organizer with the following requirements: a. IKD recorded as at the financial services authority or on the basis of the statement of claim filed in the related supervisory work unit of the financial services agency (OJK); b. is the new business model; c. have the scale of effort with a broad market coverage; d. registered in the organizer’s association and e. other criteria set by the financial services agency (OJK).

A period of organizing regulatory sandbox is the one (1) year and may be extended for 6 (six) months if necessary. During the implementation of regulatory sandbox the Organizer is obligated to fulfill the following conditions: a) Notify each IKD change owned; b) Commit to open any information relating to the implementation of the Regulatory Sandbox; c) Follow education and counseling necessary for business development in the financial services sector; d) Follow any implementation of the coordination and cooperation with the authorities or ministries/agencies; and e) Collaborate with the financial services Agency or party activities in the financial services sector.

The status of regulatory sandbox result will be: a) Recommended; b) Repair; or c) Not recommended. If recommended status is given then OJK will provide recommendations for registration in accordance with the business activities of the Organizer. If the repair status is given, then OJK will give six months extension from the date of the determination of status. If the status is not recommended then the organizers cannot resubmit the same IKD and will be issued from the recording as an organizer. Application to the financial services agency (OJK) no later than six months from the determination of the status of recommended. If it exceeds the time period then the status revoked & stated does not apply.

OJK obligatory monitoring of the entire good organizers that have not been recorded but has been operating the organizers have been recorded & registered in OJK. According to the author, efficient monitoring based on periodic reports organizer, direct monitoring, by the report of the community; OJK is obligated to conduct surveillance against: a) The ethical standards of the profession and the market; b) Transparency of products and services; c) Competitive and

inclusive market; d) Conformity with the needs of consumers; e) Handling the complaints mechanism; f) Security and confidentiality aspects of consumer data and transactions; g) Aspects of compliance with the regulations; h) Standard and security aspects of the platform; i) Information technology governance aspects; a. market risk; k. counter-party risk and clearing agency; b. aspects of online education; and m. aspects of electronic certificates.

Supervising the block-chain is required by all parties, in particular, the Ministry of communications and Informatics, Bank Indonesia, the financial services agency (OJK), the State police of the Republic of Indonesia (the national police/POLRI), the center of reporting and Financial Transaction Analysis (PPATK). The cooperation between these institutions is urgently needed to prevent block-chain based banking cybercrime. OJK is also obliged to guard consumers who suffer consumer losses to get their money back in a civil suit (Karo Karo, 2018).

The owner of the data in the block-chain system is a block-chain provider company. Therefore, the company is subject to the mandatory rules from the Minister of Informatics and Communications No. 20 Year 2016 on the Protection of Personal Data in the Electronic System (Permenkominfo 20/2016) one of which is the organizer of the electronic system the owner must respect personal data over the nature of the personal data privacy.

The protection of personal data is only in the form of Permenkominfo, hence Kominfo Minister is obliged to cracked down decisively by giving administrative sanctions to perpetrators attempt either: a) An oral warning, b) Written warning, c) Temporary activity termination, d) Announcements on a site in the network (Karo Karo, 2019).

An effort is required to cut the chain of crimes of money-laundering: with a way to foreclose and seize proceeds of crime, in addition to the relatively easy to do but it will also be able to eliminate the motivation to commit crime again (Husein, 2007). Article 23 paragraph (1) of the TPPU Law finance service provider must report to the PPATK including: a. receipt of suspicious financial transaction; b. acceptance of financial cash in the amount of at least with five hundred million rupiah or with foreign currencies whose value equivalent, which performed well in a single receipt or acceptance several times within one working day; and/or c. financial acceptance of transfer of funds to and from foreign countries.

Suspicious financial acceptance criteria is a. financial acceptance deviate from the profile, characteristics, or habitual patterns of acceptance from users of the service concerned; b. financial acceptance by users of the service are thought to do in order to avoid reporting the corresponding receipt that must be carried out by the Rapporteur trust accordance with the provisions of this Act; c. acceptance finance is done or cancel is done using treasures thought to derive from the results of a criminal offence; or d. financial receipts requested by PPATK to reported by trust the rapporteur because it involves the alleged wealth derived from the results of a criminal offence.

POJK 13/2018 set of sanctions if POJK 13/2018 is breached: a) A written warning, b) Fine, obligation to pay a certain amount of money, c) Cancellation of approval, and/or d. cancellation of registration. According to Sulistiowati, if Bank Indonesia had given permission, then that can revoke Bank Indonesia is permission and the post of Bank Indonesia has provide permission then it is the form that the State is present.

If a block-chain business actor intend to do the crime of embezzlement by weighting down as set forth in article 374 of the Indonesian Penal Code then criminal sanctions is appropriate given. Criminal law function set life civic and organized layout within the community (Prasetyo, 2018). Criminal sanctions may only be carried out if there are any additions or changes to Law. Until today ITE Law only regulate on hacking in Article 32 paragraph (1), (2) and (3) and if it violates Article 32 paragraph (1) Of the Act of ITE then threatened with imprisonment of no longer than 8 (eight) years and/or a fine of Rp 2 billion, while if the violation of article 32 paragraph (2) Of the Act of ITE then threatened with imprisonment longest 9 (nine) years and/or a fine of 3 billion rupiah, while if the violation of

article 32 paragraph (2) UU ITE then threatened with imprisonment of no longer than 10 (ten) years and/or a fine of 5 billion rupiah.

## CONCLUSION

The law and legislation regulating and protecting the digital data privacy including the protection of digital data privacy in the Electronic Transactions as a whole and particularly in the blockchain business in the Pancasila Legal System has been established.

The form of the legal protection of consumers and businessmen towards the utilization of the technology of block-chain is stipulated in the form of ITE Law, and many delegated legislation such as IKD related OJK rules, Bank Indonesia Regulation related changes digital finance, or just to create specific rules on the utilization of information technology and block-chain by the authorities. As for the content of the regulation obliged to accommodate the legality of block-chain technology service provider companies, consumer protection, the seizure of assets, the procedures for settlement of disputes in the event of a dispute, the dispute civil affairs and penal disputes officers in the PPATK, officers at the Bank Indonesia, officials at the financial services authority, the police, public prosecutors, judges linked to the Information Technology and Telecommunication, particularly in block-chain system must continue to obey the law preventing and eradicate the criminal offence using the block-chain system.

## REFERENCES

- Husein, Y. (2007). *Bunga Rampai Anti Pencucian Uang*: Bandung, Terrace &Library.
- Rizky, K.K. (2019). *Enforcement of Cybercrime Crime Law through Criminal Law: Karawaci*, Faculty of Law, UPH.
- Rizky, K.K. (2018). *Article on Banking Cyber Crimes: Opinion Column for Kompas Daily*.
- Siahaan, N.H.T. (2005). *Money Laundering and Banking Crime*. Jakarta, Pustaka Sinar Harapan.
- Prasetyo, T. (2015). *Justice with Dignity in Legal Theory Perspective: Prints I*. Bandung, Nusa Media.
- Prasetyo, T. (2017). *Legal Renewal. Dignified Justice Theory Perspective: First Matter*. Malang, Setara Press.
- (2018), *Revised Edition of Criminal Law, Ninth Printing*, Depok, RajaGrafindo Persada.
- Prasetyo, T. (2019). *Legal Research A Dignified Justice Theory Perspective. Prints I*, Bandung, Nusa Media.
- Law., & Law, T. (2020). *Dignified Justice Theory Perspective. Prints I*, Nusa Media, Bandung.
- Adrian, S. (2008). *Money Laundering Crime*. Bandung, Citra Aditya Bakti.