Cellular Phone User Personal Data Protection by Provider

Siti Rahmawati[1], Zudan Arief Fakrulloh[2]
{sitirahmawati.rf@gmail.com [1], cclsis@yahoo.com[2]}

Universitas Borobudur, Jakarta, Indonesia[1,2]

Abstract. Individual information is significant on the grounds that it includes private matters ensured by the state and the information client. This review plans to clarify the guidelines in regards to the security of individual information and the Provider in protecting the individual information of cell clients. The strategy utilized is an exact regularizing approach or regulating application. This review demonstrates the significance of information security by cell card suppliers so information spillage doesn't happen on the grounds that the Provider is the holder of the cell card purchaser's information.

Keywords: Legal Protection; Personal Data; Cellular Card Provider

1 Introduction

Every law made by the legislator was a legal answer to the community's problems when the law was enacted.[1] The development of law should be in line with the development of society so that when society changes or develops, the law must change to organize all actions that occur in an orderly manner during the growth of modern society. because globalization has become the driving force behind the birth of the information technology era.

Information technology by itself also changes people's behaviour.[2] The improvement of data innovation has made the world become borderless and caused an extremely fast friendly change. So one might say that data innovation is at present a two sided deal in light of the fact that, as well as adding to the improvement of human government assistance, progress, and development, it is likewise a powerful method for unlawful demonstrations.[3]

Acts illegal in Law Number 11 of 2008 concerning Information and Electronic Transactions, wrongdoings in data innovation are called Cyber Crimes. Digital Crime is a sort of wrongdoing identified with the utilization of data and correspondence innovation unbounded[4]. It has a vital characteristic with an engineering technology that relies on a high level of security from information submitted and accessed by internet users.[5]

In Article 35 of Law Number 11 of 2008 concerning ITE, it has been clarified that "Each individual deliberately and without freedoms or illegal controls, makes, changes, erases, obliterates Electronic Information and Electronic Documents with the point that Electronic Information as well as the Electronic Document is considered as though the information is true".

In Indonesia, there are many cases related to cybercrime (cybercrime). According to the Deputy Head of Network Monitoring and Security of ID-SIRTII/CC, Muhammad Salahudin,

MIC 2021, October 30, Jakarta, Indonesia

DOI 10.4108/eai.30-10-2021.2315766

"Currently, cases of cybercrime violations from 2014 to early April have reached around 1,000 patients. This number continues to increase every year to reach 100 per cent. In 2010 only 100 cases a year. 2011 increased by 200 patients, 2012 to 400 points. In practice in Indonesia, criminal acts using computers have always been a type of crime that is difficult to classify as a crime. Lawful issues that are regularly confronted are identified with the conveyance of data, correspondence and exchanges electronically, particularly as far as proof and matters about legitimate activities helped out through the electronic framework.

One example of a cyber-crime case occurred in Surakarta, which in its proof experienced problems in the case of breaking an email password. A person suffered losses of up to billions of rupiah because the email became a transaction tool in the company. In this case, a judge presents an expert witness, who is trusted to identify the malware planted in the victim's laptop, but the expert witness from the complainant/victim could not prove it, so that the judge acquitted the defendant.

Thus, in practice, proof in criminal law has a vital role, considering that in the Criminal Procedure Code (KUHAP), the part of evidence greatly influences judges' considerations. Every obstacle that arises makes law enforcement confused to conclude a case in Information Technology, which is in the form of digital evidence.

2 Methods

The creator conducts research utilizing an experimental standardizing approach or applied regularizing to lead an investigation of the execution or execution of positive lawful arrangements (laws) and real agreements in each specific legitimate occasion that happens in the public eye to accomplish the foreordained objectives. The information utilized in this review are essential, auxiliary and tertiary lawful materials.

In collecting data and materials relevant to this discussion, the authors use field research (Library Research). In conducting field research, the author goes directly to the field by using interview or interview techniques. An interview or interview is an oral question and answer where two or more people are face to face.

3 Discussion

3.1 Mobile Phone User Data Privacy Legal Protection

The development of the use of technology in the field of telecommunications takes place very rapidly, and this has resulted in humans having many choices in communicating. In the 1990s, humans only knew wired telephones to communicate. But along with the times, the latest discoveries and innovations in means of communication are increasing, ranging from types of cellular phones with simple features, even to very sophisticated features, all are available. In addition to their form and function, cell phones have penetrated all walks of life. Almost everyone from various economic backgrounds can use cell phones for multiple purposes.

Cellular phone users are not limited to certain ages. From children to the elderly. All are cell phone users. Based on the survey results, the number of cellular phone subscribers in 2006 was around 63 million and in 2010 increased by almost 350% to 211.1 million customers.

The increasing number of cellular phone users in the community indicates that now cellular phones are not a luxury item. The expanding number of users is directly proportional to the increase in telecommunication services. The demand for Internet services is increasing and becoming a primary need in almost all levels of society in Indonesia. The choice of Provider is also the main point in choosing it because the most important thing is the security of each customer's data.

The following are some forms of liability carried out by PT Indosat Ooredoo in the event of a system error during Provider activation Based on the results of interviews about uploaded data errors and activation failures when activating three times in a row, PT Indosat Ooredo Tegal branch said that this often happened, almost 78% of a total of 50 people claimed to have experienced system problems related to the registration of the Indosat Prime Card activation—offered by PT Indosat Ooredoo manually.

As a business entertainer, PT Indosat Ooredoo ought to make up for misfortunes experienced by shoppers utilizing these Internet administrations. This is expressed in Article 19 Paragraph (1) of Law no. 8 of 1999 concerning Consumer Protection, which states: "Business entertainers are liable for remuneration for harm, contamination, or potentially buyer misfortunes because of devouring merchandise as well as administrations created or exchanged."

Furthermore, in Paragraph (2), it is explained that: "The compensation as referred to in paragraph (1) may be in the form of a refund or replacement of goods and or services of a similar or equivalent value, or health care and or the provision of compensation following the provisions of the applicable laws and regulations." In connection with the above explanation, PT Indosat as a telecommunications operator in Article 15 Paragraph (1) of Law Number 36 of 1999 concerning Telecommunications also states that: claim for compensation to the telecommunications operator."

Data recovery is a form of compensation for unlawful acts committed by business actors. Settlement obtained due to an illegal act results from not fulfilling the following elements: There is a criminal act; There is a loss; There is a causal relationship between illegal acts and failures, and there is an error.[6]

In the Hoge Raad choice, the meaning of an unlawful demonstration abuses the law and disregards the abstract freedoms of others, ethical quality, and public request. As indicated by the Decision of Hog Raad 1919, what is characterized as an unlawful demonstration is to do or not accomplish something that abuses the freedoms of others, is in opposition to commitments, is in opposition to tolerability, is in opposition to the precision that should be regarded in the public eye.[7]

An unlawful act only occurs when a business actor is declared to have failed to fulfil his obligations, or in other words, a criminal act exists if the business actor cannot prove that he has committed an illegal act beyond his fault.

The legitimate premise in regards to unlawful demonstrations and pay because of illicit demonstrations is likewise contained in Article 1365 of the Civil Code as follows: "Each act that abuses the law, which carries damage to someone else, obliges the individual who on account of his error to give the misfortune, remunerate the misfortune."

Losses experienced by customers due to unlawful acts committed by PT Indosat Ooredoo. PT Indosat through Customer Service provides compensation in the form of refunds according to the price of the previously activated package.

The refund referred to above can only be received by the customer if the complaint and the inclusion of previous evidence submitted to Customer Service through social media (*Twitter*), contacting the complaint number, or verification by email by PT Indosat Ooredoo.

However, based on user data that the author has examined regarding complaints of problems with HP interference, provider signals during registration, or data leaks by hackers or specific individuals, who have been complained about through Customer Service, complaints are responded to and will recover data.[8] Furthermore, the researcher provides an answer column that can be written by the respondent himself, with the aim that the respondent can give an explanation related to complaints related to disturbances in the registration package activation system or PT Indosat Ooredoo internet.

The following are some of the answers from respondents that the researchers managed to collect. At the same time, at the Indosat Ooredoo office, Tegal Branch, including "Customers are often blamed for technical procedural reasons when registering for package purchases, even though customers understand the process of registering a purchase for Data Security registration very well. -Student"

"According to researchers, it is not optimal because Indosat is not responsive and allows customers to wait for an extended period in the settlement process, even days to 1 week, and finally, customers have run out of time and money because of the system error. With this incident, it should be reported to the authorities who serve consumer complaints to protect consumer rights so that mistakes do not occur that can harm customers. -Employee"

The Provider has not provided the right solution in the compensation process for the loss of the quota that the customer purchased. The Provider in providing compensation requires a time-consuming process because of system disturbances.-Students"

"The services provided take a long time. So the rights of customers have not been fully protected properly. From the provider side, customer satisfaction must be prioritized.-Students"

The statements above are some of respondents' responses regarding the services of PT Indosat Ooredoo in solving problems, so users have to wait some time for the return of compensation and repair of the system. This reality goes against the guideline concerning the obligation of business entertainers under Article 19 of Law Number 8 of 1999 concerning Consumer Protection which expects pay to shoppers who are hurt. In the interim, Article 4 of Law Number 8 of 1999 concerning Consumer Protection solidly ensures the privileges of purchasers as expressed in Letter A, which says that customers reserve the option to solace, security, and wellbeing in devouring labor and products. Then, at that point, the letter G says that the option to be dealt with or served accurately and truly and not biased. Besides, it is additionally shown in letter H that purchasers reserve the option to get remuneration, pay, as well as substitution if the products or potentially benefits got are not after the understanding or not as they ought to be.

Based on complaints from respondents that the researchers collected, also based on other sources to support evidence of consumer complaints related to errors in the Internet service system, especially on the activation of packages offered by PT Indosat Ooredoo. This proves that Indosat is proven to have violated the legal rules that the researcher has described above. Indosat as a business actor, must be responsible and provide compensation to consumers whose rights have been injured based on the legal rules specified in Article 7 letter F of Law Number 8 of 1999 concerning Consumer Protection.

3.2 Provider's Policy on Protection of Provider Card User's Personal Data

Supplier arrangements on Personal Data Protection for every supplier card client are typically unique at the organization's approach, in this manner ordinarily, candidates from supplier cards not set in stone dependent on broad arrangements that are required and outright

(as laws and guidelines that the public authority has set) and adaptable guidelines (rules made by the supplier organization) which incorporate the treatment of client data, including actually recognizable data got by the Provider, and data got when the client utilizes the offered support supplier.[9] This Privacy Policy doesn't matter to the acts of organizations that are not claimed or constrained by the Provider or people who are not utilized or driven by the Provider, including outsider suppliers.[10]

To protect data that is feared to be misused, the Minister of Communications and Information Rudiantara explained that the prepaid card re-registration policy limits one person with an e-KTP Population Identification Number (NIK) to only having three SIM cards. For people who have businesses, one of the numbers must be deactivated to be used properly.[11] For this situation, there is now a Regulation of the Minister of Communication and Information Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems.

"For sure, the public authority is planning, Kominfo is setting up a Personal Data Protection Bill which will be remembered for the National Legislation Program (Prolegnas). We will propose for 2018".

This policy is needed. The Minister of Communication and Information Technology 20/2016 becomes a reference because it is needed. Because it can help users feel safe and comfortable with every service provider action to users the Indonesian people who have entered the digital era are required to have a law that regulates the security of provider card user databases.

According to Mr Herman as Head of Legal Bureau of Indosat Tegal area, said that "Although we strive to protect Personal Data, we emphasize that consumers take precautions to protect Personal Data, namely by changing passwords frequently, using a combination of letters and numbers, and ensuring that You are using a secure browser."

The Provider might acquire different kinds of data about the client or the client's cell phone gadget, which might incorporate data that can be utilized to recognize the client as characterized as follows: User-Provided Information: The client gives specific Personally Identifiable Information, for example, cell phone number, pop-up message name (assuming any), charging data (assuming any) and client's cell phone data to the Provider when deciding to partake in the utilization of the Service, for example, enlisting as a client; Log File Information: When the User utilizes the chose Service, the Provider's server naturally records specific data on the client's internet browser when sending at whatever point the client visits any site that can show the desires, propensities, top choices of the client and any data identified with the client. Server records might incorporate data, for example, the client's web demand, Internet Protocol (IP) address, program type, program language, alluding page and URL, stage type, number of snaps, area name, the principal page of the site, pages saw and the request for those pages. The measure of time spent on a specific page, the date and season of the client's solicitation, at least one treats that can extraordinarily recognize the client's program, the client's telephone number.

The supplier might give individual distinguishing proof data or non-individual ID data to outsider specialist organizations as long as it is sensibly important to perform, fix or keep up with the Provider's card Services. The supplier might share non-individual recognizable proof data, (for example, mysterious User use information, alluding pages and URLs, stage type, resource visits, number of snaps, and so forth) with intrigued outsiders to help Provider in understanding client propensities on the Service from the Provider's card.

The supplier might gather and delivery actually recognizable data and non-by and by recognizable data whenever needed to do as such by law, or in the great confidence conviction

that such activity is important to follow public law, worldwide law or in light of court requests, summons, or looking for ensures. Or on the other hand the same, or then again if in sensible certainty, the actual security of an individual could be put in danger or compromised.[12]

The Provider additionally has the option to uncover individual ID data and non-individual distinguishing proof data which the Provider considers in sincerely suitable or significant to do the Terms and Conditions of Service, to play it safe against responsibility, to explore and guard against any outsider cases or requests, to help government law requirement offices, to ensure the security or uprightness of Service Providers, and to ensure the freedoms, property, or individual wellbeing of Providers, administration clients or others.[13]

The supplier utilizes physical, administrative, and specialized protections to keep up with the uprightness and security of Users' own data. Notwithstanding, the Provider can't guarantee or ensure the security of any data sent by the client at the client's own danger. It is firmly debilitate to utilize unstable wifi or unprotected organizations. After the Provider gets conveyance of data from the client, the Provider will economically try to guarantee the framework's security. In any case, this isn't an assurance that the information can't be gotten to, uncovered, adjusted, or obliterated due to disregarding any arrangements of the actual Provider.

If the Provider becomes mindful of a security framework break, the Provider might endeavor to advise the client to go to proper preventive lengths. The supplier might post a notice in case of a security break. This Privacy Policy might be amended intermittently and reflected by the "last update date". The client's proceeded with utilization of the Service is considered to be the client's agree to the Privacy Policy. The Provider gives solidness to every client prior to approving info with respect to individual information, either carefully composed (for electronic data through web media), or recorded as a hard copy for the people who approve physically: "Client Expressly Admits That User Has Read Terms and Conditions of Service This As Well As Understanding The Rights, Obligations, Terms And Conditions That Are Arranged In Our Services."

4 Conclusion

Customers who experience problems with their provider card can complain to PT Indosat Ooredoo through Customer Service so that customer complaints can be immediately followed up. In the process of giving responsibility to customers who are harmed, PT Indosat Ooredoo first checks and asks the person in charge of the API (application programming interface), which is a technology to facilitate the exchange of information or data between two or more software applications, whether there is If there is a problem with Indosat Ooredoo's data package or not, if there is a problem, then PT Indosat Ooredoo as a business actor and telecommunication service provider guarantees that the data will be safe.

Supplier's approach on ensuring individual information of supplier card clients uses such Personally Identifiable Information to work, keep up with, and give clients the elements and elements of the chose Service. Suppliers utilize physical, administrative, and specialized shields to keep up with clients' very own data trustworthiness and security. In the event that the Provider is aware of a security framework break, the Provider can attempt to advise the client to make suitable preventive strides.

References

[1] E. E. Supriyanto, M. Rachmawati, and F. J. Nugroho, "Transformative Policies and Infrastructure Strengthening Towards the Police Era 4 . 0," *J. Bina Praja*, vol. 13, pp. 231–243, 2021.

[2] E. E. Supriyanto, "Kebijakan Inovasi Teknologi Informasi (IT) Melalui Program Elektronik Goverment dalam Meningkatkan Kualitas Pelayanan Publik di Indonesia," *JIP (Jurnal Ilmu Pemerintahan) Kaji. Ilmu Pemerintah. dan Polit. Drh.*, vol. 1, no. 1, pp. 141–161, Apr. 2016, doi: 10.24905/jip.1.1.2016.141-161.

[3] J. Dixon and R. Dogan, "Hierarchies , Networks and Markets : Responses to Societal Governance Failure," *Adm. Theory Prax.*, vol. 24, no. 1, pp. 175–196, 2002.

[4] *Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*. .

[5] D. E. Holmes, *Big Data: A Very Short Introduction*, vol. 1, no. 1. Oxford University Press, 2017.

[6] P. El Harry and R. Riswadi, "Cyber Crime Hate Speech Criminological Review in 2018-2019 (Case Study in Salatiga City)," vol. 2019, 2021, doi: 10.4108/eai.6-3-2021.2306883.

[7] B. Fachriandi and T. Dirgahayu, "Kepedulian Keamanan Informasi di Pemerintahan: Praktik Manajemen dan Dampaknya," *J. Manaj. Inform.*, vol. 11, no. 1, pp. 72–87, 2021, doi: 10.34010/jamika.v11i1.4584.

[8] C. S. Hutchinson and D. Treščáková, "The challenges of personalized pricing to competition and personal data protection law," *Eur. Compet. J.*, vol. 0, no. 0, pp. 1–24, 2021, doi: 10.1080/17441056.2021.1936400.

[9] C. Affonso Souza, C. César de Oliveira, C. Perrone, and G. Carneiro, "From privacy to data protection: the road ahead for the Inter-American System of human rights," *Int. J. Hum. Rights*, pp. 147–177, 2020, doi: 10.1080/13642987.2020.1789108.

[10] H. Ha, H. S. Loh, H. T. E. Gay, and P. F. Yeap, "Consumer protection in E-tailing computer sales: a case study of Dell," *Int. Rev. Law, Comput. Technol.*, vol. 0, no. 0, pp. 1–24, 2020, doi: 10.1080/13600869.2020.1838187.

[11] C. Handoko, "Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime Di Pengadilan," *J. Jurisprud.*, vol. 6, no. 1, p. 1, 2017, doi: 10.23917/jurisprudence.v6i1.2992.

[12] L. B. Moses, F. Johns, and D. Joyce, "Data associations in global law and policy," *Big Data Soc.*, vol. 5, no. 1, p. 205395171878343, 2018, doi: 10.1177/2053951718783438.

[13] A. D. Dixon, "The Strategic Logics of State Investment Funds in Asia: Beyond Financialisation," *J. Contemp. Asia*, vol. 00, no. 00, pp. 1–25, 2020, doi: 10.1080/00472336.2020.1841267.