Online Transportation: Violation of Privacy Rights and Vulnerability to Sexual Violence by Drivers in Digital Platform-Based Work

Hernawan Hadi¹, Kukuh Tejomurti², Mochammad Najib Imanullah³, Nurhidayatuloh⁴
¹,₂,³ Universitas Sebelas Maret, Surakarta - Indonesia
⁴Universitas Sriwijaya, Palembang - Indonesia
kukuhfhuns@gmail.com

Abstract—This study will examine the relation of the lack of protection of consumers’ digital personal data online transportation modes which have implications for the vulnerability of sexual violence carried out by drivers of online transportation. The annual data of the Women’s National Commission in 2019 shows there were 406,178 cases of violence against women in 2018. Among these cases, there were at least 2-5 percent of cases of sexual violence in the mode of online transportation. Sexual violence is not a statistical problem; one case is that an increasing number of crimes indicate that there is a serious problem with the protection of the personal data of consumers of online transportation. This study uses normative legal research that is prescriptive. The results of the study indicate that firstly, the majority of online transportation drivers still have not received education about consumer rights, especially women who are vulnerable to acts of sexual violence. Second, the recruitment and track record of drivers is still not done well by online transportation application providers. Third, the application providers have made repressive efforts against individual drivers who acted in crime despite still not being fair because the treatment of victims seems to be still not responsive.

Keywords—Online Transportation, Sexual Violence, Violation of Privacy Right

1. INTRODUCTION

In 2017 it was noted that at least more than 3,885,567,819 people around the world used internet technology. The penetration reaches 51.7% of the total population in the world that has exceeded 7.5 billion. The data of World Internet Usage and Population Statistics as of June 30, 2017, the Asia Continent recorded having the highest internet users, namely 1,938,075,631 users with penetration reaching almost 50% including Indonesia, there were 1,132,700,000 users [1].

Data from the Indonesian Internet Service Users Association or Asosiasi Pengguna Jasa Internet Indonesia (APJII) also notes that Indonesia is a country that has the 8th largest internet user in the world and the 4th largest in Asia. Internet users in Indonesia reached 132.7 million users consisting of 52.5% male users and 47.5% female users with the highest users on Java Island at 86.3 million users [2].

<table>
<thead>
<tr>
<th>World Regions</th>
<th>Population</th>
<th>Internet Users (30 Jun 2017)</th>
<th>Penetration Rate (% Pop.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>1,246,504,865</td>
<td>388,376,491</td>
<td>51.2%</td>
</tr>
<tr>
<td>Asia</td>
<td>4,148,177,872</td>
<td>1,938,075,631</td>
<td>46.7%</td>
</tr>
<tr>
<td>Europe</td>
<td>822,710,362</td>
<td>659,634,487</td>
<td>80.2%</td>
</tr>
<tr>
<td>Latin America/Caribbean</td>
<td>647,604,645</td>
<td>404,269,163</td>
<td>62.4%</td>
</tr>
<tr>
<td>Middle East</td>
<td>250,327,574</td>
<td>146,972,123</td>
<td>58.7%</td>
</tr>
<tr>
<td>North America</td>
<td>363,224,006</td>
<td>320,059,308</td>
<td>88.1%</td>
</tr>
<tr>
<td>Oceanasia/Australia</td>
<td>40,479,846</td>
<td>28,180,356</td>
<td>69.6%</td>
</tr>
<tr>
<td>World Total</td>
<td>7,519,028,970</td>
<td>3,885,567,619</td>
<td>51.7%</td>
</tr>
</tbody>
</table>

Source: Internet World Stats, 2017

Information and communication technology simultaneously has formed patterns of behavior and lifestyle of the community. The pattern of relationships borderless in the social, cultural, economic, and law enforcement fields that take place so quickly is due to the development of information technology. Information technology in addition to providing a positive impact on human beings, can also be used as an effective tool in carrying out acts against the law [3].

One of the uses of internet technology that is now developing is the emergence of transportation modes that are integrated with smartphone-based applications or which are often called motorcycle taxis and online taxis. The phenomenon of disruption of information technology aims at sharing the economy that has grown in the last five years [4]. One of them is the development of public transportation by utilizing internet technology, such as Go-Jek, Blue Jeh, Grab, Uber, and so on. According to data as of November 2017 it was found data that 2 (two) companies such as Go-Jek and Grab had significantly increased users. Go-Jek has a user base of 8.8 million, Grab has a user base of 8.6 million. Regarding the
number of users by sex. Go-Jek has 3,403,000 male users and 5,468,000 female users. Whereas Grab has 4,259,000 male users and 1,355,000 female users [5]. Urban residents as users prefer to use transportation applications online than transportation conventional because there is no need to bargain, not afraid to be cheated, no need to wait too long and look for online transportation vehicles, just order and wait for the transportation vehicle online will contact and come to users [6].

In addition to offering various service features that are beneficial to consumers, on the other hand it also raises many problems from competition between conventional online transportation and public transportation, alleged violations of consumer data privacy by drivers and applicator companies, to the sexual violence of consumers of online transportation by using personal data stored conducted by individual drivers [7].

The massive provision of private data distribution that is privacy in applications that use the internet in the era of digital technology is a necessity. Urban residents who are busy working in the office and have no time to buy lunch, hence the use of online transportation features that offer purchasing and food delivery services is a necessity. The interest in shopping for urban people who switched from conventional stores to online shop (e-commerce) also increased significantly. For instance, online store Bukalapak has been recorded 35 million users (monthly active users) and the number of transactions reaches 320 thousand transactions per day, which are spread throughout almost all regions of Indonesia [8].

An important issue arises about the protection of personal data of online transportation consumers in urban residents who tend to be massive to provide their personal privacy data to online transportation application providers without accompanied legal certainty over consumer personal data. Personal data such as: name, address, e-mail, and the user's personal mobile number will be stored automatically or manually (through screenshots) on the applicator and third parties such as drivers or other parties if interested in the consumer's personal data.

Several cases about sexual violence against women in online transportation still occur since this kind of system developed in Indonesia. The following are few examples notes that provided by Women National Commission concerning sexual violence cases carried out by online transportation drivers to consumers in alleged use of women’s victim personal number:

<table>
<thead>
<tr>
<th>No.</th>
<th>Year</th>
<th>Case</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2016</td>
<td>Senior High school female student got sexual violence chat and threaten to know the location of the school and the victim's house if they do not fulfill the driver's request</td>
<td>Jakarta</td>
</tr>
</tbody>
</table>

According to the data collected from Women National Commission, it is indicated that the security of online transportation consumer privacy data is still low by the reason it could be misused by the drivers, for instance: the Drivers are still able to reach the consumer through Whatsapp Application or Short Messages Services (SMS). Rights issue of Privacy is still an issue because related with the protection of Human Rights provided in Universal Declaration of Human Rights issued by United Nations whereas stated that [9]:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”.

Furthermore, pursuant to Article 28 G of The Indonesian 1945 Constitution stated that:

“Everyone has the right to personal, family, honor, dignity and property under his control, and has the right to security and protection from the threat of fear of doing or not doing something that is a human right”

Joe Cannataci stated that if someone feels his privacy data is well protected, then that individual will have the choice to live a life based on motivation and reason authentically, not the result of manipulation or pressure from other parties [10]. Concern over violations of the right to privacy is important because in the context of the life of the state, the right to privacy of citizens is mandatory.

The assessment of the relationship between the privacy of personal data that is private from consumers of online transportation with the vulnerability of sexual violence is needed to be explored to help describe the “causes, consequences, and solutions” that occur between them.
II. RESEARCH METHOD

This study is a normative legal research that is prescriptive in nature by order to describe the complexity of the current problems. Data collection is done through library research and field research and the library research stage is conducted to find secondary data using primary, secondary, and tertiary legal materials. In this study also describes the vulnerabilities that arise from the openness of personal data of online transportation consumer which driven by the application platform. Data collection is carried out in stages and through document studies by researchers by tracing various journal articles, government reports, research reports, and institutional reports related to the topics being studied.

Data analysis is done qualitatively. The analysis starts from data collection, this data is then presented by means of selecting, classifying systematically, logically and juridically to find out the specific description related to the problems in the research, after which the author makes an interpretation or interpretation. Then the authors compare with the theory and concepts of secondary data consisting of scientific books, journals, and related legislation and legal opinions from legal experts.

III. FINDINGS AND DISCUSSION

1. The Concept of Privacy Right

Personal Data protection as one of the human rights affect countries in the world to stated that personal data protection should be consider as their constitutional right or in other words “habeas data” that human rights to obtain protection of his/her own personal data against a violation and to fix several fallacies of his own data. Portugal is a country that consider data protection as constitutional rights. According to ASEAN Declaration of Human Rights also consider privacy rights.

Currently, more than 75 countries which consider personal data protection under their legislation [11]. Including in Argentina, Law concerning Electronic Document and Personal Information Protection in Canada, Japan, India, South Korea, Singapore, and Philippine.

In the European Union, data protection and privacy for all individuals in Europe and the European Economic Area are regulated in the General Data Protection Regulation (GDPR). GDPR aims to provide EU citizens and citizens with oversight of personal data, and to simplify the regulatory scope for international business. Affiliated companies under the European Union must have higher standards in terms of maintaining data protection and privacy. Companies that violate GDPR can be subject to sanctions of up to 20 million Euros. India is one country that has been exposed to GDPR sanctions. In 2010, India still did not have sufficient standard rules in terms of data protection and privacy so there were restrictions on the export of personal data from European Union member countries. In the end, therefore India and the European Union have formed Expert Groups from both parties to discuss how to form sufficient protection [12].

Regarding privacy, according to Ann Covoukian, privacy can be in the form of the right to control information about one's person and the ability to determine in terms of what and how to obtain and use that personal information.

There are three elements of privacy [13]: First, privacy about individual, which is based on the general principle that everyone has the right to be alone. From privacy about individual, there are four kinds of violations, among others. 1) Appearance that puts someone in a place that he is not supposed to be in. For example, by using a photo of a man on an illustrated picture of domestic violence; 2) Public appearance of one's name or hobby to get economic benefits; 3) Publication of embarrassing personal information to the public; 4) Interfering with one's solitude. Second, Privacy of data about person, right which binds to information about someone that collected and used by others, such as: information about medical records, habits of a person, political party membership, tax information, insurance information, criminal information. Misused of information collected from consumers or customers can be a violation of a person's right to privacy. Third, privacy for someone's communication conducted in online communication. Under certain conditions, the supervision and disclosure of the contents of electronic communication by other people not by people who own it directly or the person which it is sent can be categorized as a violation of a person's right to privacy.

Protection of human rights in international law, protection of the privacy right is regulated pursuant to Article 12 of the General Declaration of Human Rights (UDHR) 1949 which states that:

"No one shall be subject to arbitrary interference with his privacy, family, home or correspondence, to attack upon his honor and reputation. Everyone has the right to the protection of such interference or attacks.

Protection of the right to privacy is also affirmed through arrangements in the International Convention on Civil and Political Rights (ICCPR) Article 17 which states that:

(1) No person may be arbitrarily or illegally interfered with personal matters, his family, his home or correspondence, or illegally attacked by his honor and reputation;

(2) Everyone has the right to legal protection against interference or attacks as mentioned above;

According to Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia also states that:
Everyone has the right to personal, family, honor, dignity and property under his control and has the right to security and protection from the threat of fear to do or not do something that is a human right.”

According to Article 28G paragraph (1), it can be explained that every Indonesian citizen has the right to privacy of data about data person, namely the rights attached to information about an individual that is collected and used by other people. Neglecting the right to privacy of data about person can potentially violate the constitutional rights of citizens [14].

2. Collection of Personal Data Users of Online Transportation

In application-based online transportation, consumers are practically placed in positions that do not have the choice to approve or disagree (the concept of consent) a privacy policy regarding the collection, processing and storage of the personal data they provide. The concept of consent or agreement is the basis for building trust in the middle of the information technology era. In the concept of relations online, this concept is very fundamental, but in practice it is difficult to establish a balanced relationship between owners and data collectors, resulting in violations of the right to privacy of consumers [15].

In the practice of registering users as consumers of online transportation, a warning is found in the form of a standard with substance that is very difficult to understand, length and form of writing that is too small to put the user in a position that has no other choice to approve even though the consequences have long-term consequences. Therefore, at the International Conference of Data Protection and Privacy Commissioners (ICDPPC) meeting 39th in the Faculty of Law, Hong Kong University questioned the method of consent or approval of the complicated privacy policy notification [16]. No longer being effective in establishing a balanced relationship between the openness of personal data on online transportation with the right to privacy.

According to Kukuh Tejomurti's research on the two online transportation privacy policies in 2018, information can be taken that first, the online transportation applicator collects consumer personal data in a big data applicator company; secondly, third parties, such as drivers after completing their duties, are likely to save in any way the consumer's personal data information. Especially in the Gojek application: there is a provision that the applicator is not responsible for actions taken by the service provider / driver, and the customer agrees to defend, not claim compensation, and free the applicator from all responsibilities; third, the customer's personal data can be transferred, stored, used and processed in a jurisdiction other than Indonesia where the applicator company's servers are located; fourth, especially on the application of Grab Group, the customer's personal data information can be transferred, assessed or disclosed to third parties both domestically and abroad for additional purposes and objective.

3. Violations of Privacy Rights and Vulnerability to Sexual Violence by Drivers of Online Transportation

Consumer data has been shared by users of online transportation applications include: name, face, home address, location, place of work, and user ID. The openness of access to the customer's personal data is vulnerable to the potential for the determination of the time the customer goes to work, home from work, daily routes, home atmosphere, and workplace conditions. All these determinations can be used by criminal individuals to commit acts of crime, robbery, rape or simply sell important data to other parties. To this issue, there are currently no specific governance arrangements to protect digital personal data of customers in the online transportation mode.

Another vulnerability is that applicators can find out trends and interests in using application features. This information can potentially be used for certain product business objectives that are not desired by the customer. Vulnerability violations of the right to privacy of online transportation users can also occur because a service provider / driver can indirectly have access Whatsapp customer. Therefore, service providers / drivers can use the customer's personal data outside of online transportation services without permission from the owner of personal data that should be protected by confidentiality.

The openness of personal data of consumers of online transportation users has relations with the existence of acts of sexual violence against users, especially women. The definition of sexual violence is any act of gender-based differentiation that results in or may result in physical, sexual, or psychological misery or suffering, including the threat of such acts, coercion or deprivation of arbitrary freedom, both in the public sphere and in personal life [17].

One of the acts of violation of the right to consumer privacy is the determination of the time the customer leaves for work, after work hour, daily route, home atmosphere, and the condition of the workplace, storage and use of the consumer's mobile number not in accordance with the objectives, including:

a. a driver contacts the consumer and takes a profile photo of the consumer Whatsapp or Line consumer application and is placed in the pictures, sent to the user's consumer, and gets the threat to be disseminated on social media to be negative;
b. a driver contacts consumers of users who have been served and sends chats containing sexual violence;

c. Collection of habitual activities for consumers of online transportation users who are then used by unscrupulous drivers without the purpose of online transportation applications;

Pursuant to Article 26 of Law Number 19 Year 2016 concerning Amendment to Law Number 11 Year 2008 concerning Electronic Information and Transactions, states that:

1) Unless otherwise stipulated by legislation, the use of any information through electronic media relating to one's personal data must be carried out with the consent of the person concerned;

2) Everyone ... and so on;

Meanwhile according to Article 21 of the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Electronic Personal Data states that: Displaying, announcing, sending, distributing, and/or opening access to personal data in electronic systems can only be done:

a. Upon approval unless specified otherwise by the provisions of the legislation;

b. After verifying accuracy ... and so on;

Third parties such as service provider’s /delivery drivers who utilize and process customer personal data outside of service transactions according to online transportation applications and without the approval of personal data owners, namely customers / users, potentially violate the right to privacy of customers / users of online transportation. Although in the registration of online transportation applications the user has agreed to a privacy policy, but it does not mean that third parties such as drivers can utilize and process customer personal data because users only give approval with online transportation applicators as providers of electronic systems not with third parties such as: drivers or companies - other third party companies such as marketing companies, sponsoring companies and advertising.

The efforts of online transportation service providers to operate online transportation services are also considered to be still not gender friendly and provide assurance of the protection of the user's personal data protection. As for the actions of online transportation application service providers in the form of:

a. Verify prospective driver documents and check the background of prospective drivers;

b. Prospective driver recruitment requires Photos of Resident Identity Card (Kartu Tanda Penduduk/KTP), Vehicle Completeness Letter;

c. Police Record Certificate (Surat Keterangan Catatan Kepolisian/SKCK);

d. 'Matching' program between female drivers and female consumer users;

e. The application provider can suspend individual drivers who commit acts of violation of the rights to the privacy of consumers of users;

According to Olin Monteiro (female activist from Jakarta Feminist Group Discussion (JFDG), Online transportation cannot simply ask survivors to come and complain about the violence experienced. Victims may be traumatized so they need comprehensive counseling assistance. Victims can only speak in time when they are ready to talk. Application service providers can show empathy to all victims by coming home, providing counseling, taking closed testimony, and can even be accompanied by organizations that focus on women such as the Legal Aid Institute (LBH).

According to Anindya Vivi (Hollaback Jakarta) states that sexual violence is not new because more than 300 stories submitted to the website or Hollaback application are sourced from online transportation, suspension of drivers as an effort that will not be enough to stop the behavior of sexual violence. If other drivers also have the same behavior is a futile action. Application providers should conduct tighter screening and also provide education about sexual violence. This not only protects passengers because we know that many drivers of online transportation are women who have the potential to get sexual violence from their fellow partners and passengers.

IV. CONCLUSION

Vulnerability violations of the right to privacy of online transportation users can also occur because a service provider / driver easily obtains consumer personal data such as: geolocation of home and work place, and user's mobile number where the number mobile user/s is also connected with whatsapp or line user application so that the provider service / driver can indirectly have access whatsapp customer. Therefore, service providers / drivers can use the customer's personal data outside of online transportation services without permission from the owner of personal data that should be protected by confidentiality.

Sanctions for suspension of drivers who commit sexual violence due to the use of customer data that are not suitable for their customers are not enough because the victim is even more traumatized when outside the house because drivers can threaten, suppress, and terrorize victims. Moreover, the victim's telephone number is already known by the driver. Suspension sanctions need to be followed by other efforts including: improving the security of the application system such as the panic button that can be connected with the police when in an emergency, legal and psychological assistance, a more rigorous recruitment process, and a driver's code of ethics for consumer’s users especially women.
REFERENCES


[2] APJII, Survey Results: Penetration and Behavior of Indonesian Internet Users, [Indonesia Polling 2016], p. 3


[17] Declaration of Abolition of Violence Against Women, Article 1