International Seminar of Research Month 2021
Volume 2022
http://dx.doi.org/10.11594/nstp.2022.2417

Conference Paper

Criminal Liability in Cases of Personal Data Leakage Amid the Covid-19 Pandemic

Eka Nanda Ravizki*

Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya 60294, Indonesia

**Corresponding author:*
E-mail:
eka.nanda.ih.@upnjatim.ac.id

ABSTRACT

Recently, there was an alleged leak of personal data on the Electronic Health Alert Card (eHAC) application. The eHAC application is an application to verify passengers traveling during the Covid-19 pandemic. A report found experiencing the alleged leak of 1.3 million personal data users of the application. Meanwhile, the leaked data that can be retrieved from the eHAC database includes personal data of application users, including names, ID card numbers, passports, profile photos, and hotel details of users. In addition to personal data, documents on Covid-19 test results can also be accessed. For example, data from hospitals to clinics entered in the eHAC application, hospital details to the coordinates of the hospital location. Seeing this case, the issue of security in the management of big data becomes essential. Moreover, those big data is sensitive and significantly needed in handling the Covid-19 pandemic. In addition, the issue of who is the most criminally responsible for the leakage of personal and sensitive data also needs to be discussed so that similar cases do not occur in the future. Thus, this research paper aims to understand the legal concept of criminal liability in personal data protection and policy challenges in Indonesia. The research used doctrinal-comparative legal research, which desk study research, and qualitative method. As a result, the research found the possible models of criminal liability in cases of personal data leakage. Yet, the Indonesian government faces several challenges in implementing the concept of a personal data protection policy. Therefore, there is a need to propose how future policies related to personal data protection can be implemented in Indonesia.

Keywords: Criminal liability, big data, Covid-19

Introduction

The public has recently been shocked by the alleged leak of 1.3 million personal data of electronic Health Alert Card (eHAC) users. This issue has attracted the attention of many people because the application has been used to track Covid-19 in fulfilling flight requirements. eHAC is a Health Alert Card, a modern version of the previously used manual card developed by The Ministry of Health. The discovery of the eHAC user data leak was first discovered by vpnMentor researchers. Reporting from vpnmentor.com, 1.3 million eHAC user data was found on a server that everyone can access. These findings make eHAC user data very vulnerable to misuse, as for some of the leaked data, including names, home addresses, ID numbers, hospitals where Covid-19 tests were carried out, and so on. In addition to personal data, documents on Covid-19 test results can also be accessed. For example, data from hospitals to clinics entered in the eHAC application, hospital details to the coordinates of the hospital location.

In addition to alleged data leaks in the eHAC system, there are similar cases involving platforms/applications from the government related to handling Covid-19. For example, the PeduliLindung application developed by the government for the handling of Covid-19 has not

How to cite:
Ravizki, E. N. (2022). Criminal liability in cases of personal data leakage amid the covid-19 Pandemic. *International Seminar of Research Month 2021*. NST Proceedings. pages 91-95. doi: 10.11594/ nstp.2022.2417

been fully able to protect the personal data of its users. The proof is that recently the vaccine certificate belonging to President Joko Widodo, which was included in the application, was spread after the presidential NIK was widely circulated in cyberspace. Similar leakage events are very likely to occur in other residents.

There are several sources of causes in cases of alleged eHAC and Pedulilindungi data leaks. First, the ease of data theft due to the negligence of the developer/vendor and the institution or company as the data guardian involved in the application service. Second, the government's digital security system infrastructure does not yet have reliable data security protocols. Third, the impact is personal data which is a collection of information containing a person's identity. So when the information is managed haphazardly and leaked, data owners will be vulnerable to becoming victims of cybercrimes and real daily threats.

In the case of alleged eHAC and Pedulilindungi data leaks and previous data leaks, it proves that the Electronic-Based Government System (SPBE) is not working correctly. Therefore, the privacy and protection of personal data need to be a concern in the implementation of SPBE. Furthermore, the current digital era presents challenges to the privacy integrity of personal data. One of the things that makes the digital age a challenge to the privacy of personal data is the nature of digitized information which encourages the formation of an environment that does not respect the confidentiality of personal data, considering that personal data becomes easy to collect and disseminate. In addition, the issue of data portability is also a challenge in itself, where currently cloud computing technology is increasingly being used, including by government agencies, to store various data, including personal data (Chandra, 2021).

Seeing this case, the issue of security in the management of big data becomes essential. Moreover, those big data is sensitive and significantly needed in handling the Covid-19 pandemic. In addition, the issue of who is the most criminally responsible for the leakage of personal and sensitive data also needs to be discussed so that similar cases do not occur in the future. Thus, this research paper aims to understand the legal concept of criminal liability in issues related to personal data protection and how future policies related to personal data protection can be implemented in Indonesia.

Material and Methods

This study uses a normative legal research method that emphasizes library research on secondary data, with descriptive analysis and evaluative and prescriptive forms. Three approaches are used in answering the issues raised, namely the legal, conceptual, and comparative approaches. The conceptual approach is used primarily to answer the first problem regarding the concept of criminal liability in cases related to personal data protection. Meanwhile, the three approaches are used to answer the second problem regarding the dynamics of personal data protection arrangements associated with the implementation of the Electronic-Based Government System (SPBE).

Results and Discussion

The concept of accountability

The collection, use, and management of public data by the State is a necessity. In addition, in the SPBE Master Plan, as attached to the SPBE Presidential Regulation, there are efforts to utilize various new technologies such as big data, IoT, and AI, where some examples of these technologies use data and information owned by government agencies or the State as fuel, for these technologies to work. However, the problem is that massive collection and processing of individual community data, especially by government agencies, is considered not in line with the traditional concept of the right to privacy which is intended to protect individuals by giving individuals the right to control their personal information.

Thus, the massive collection and processing of individual community data still create discourse, significantly when it is associated with human rights and the state's obligation to

protect the personal rights of its citizens. Therefore, if there is an error, either dolus or culpa, committed by a government agency, the question arises as to the extent of responsibility that the government agency must fulfill. Furthermore, if it is associated with criminal liability, how can the concept be applied if the interpreter is a government agency.

Failure to protect personal data is regulated in Permenkominfo Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems—both private sector and public services. Therefore, responsibility is not only borne by third parties as application providers but also ministries or agencies controlling and processing data. The sanctions are verbal warnings, written warnings, up to the revocation of the applicable license, or being blocked. However, of course, this condition cannot be done immediately. Plus, so far, no precedent has said the Ministry of A gives a reprimand or verbal warning to the Ministry of B.

There is a fact that based on the results of the police investigation, the perpetrator suspected of leaking data is an administrative staff at one of the urban village offices in Jakarta to access the PCare system so that they can make vaccine certificates and connect to the PeduliLindung application, without going through the correct procedure and without the need for vaccinating. Thus, according to the police/government, this incident was not a data leak but an abuse of authority. Assuming that seems to make this case stop in the administrative realm because abuse of authority is regulated in Law Number 30 of 2014 concerning Government Administration, where the sanctions are also not too significant. Therefore, in another sense, it can assume that the government seems to consider this only an administrative problem that is not so serious.

On the other hand, based on the reference from practice in Europe, according to the EU General Data Protection Regulation (GDPR) or the General Data Protection Regulation in European Union law, the incident of eHAC leakage is indicated to be a severe violation. This is because the data security system does not meet the privacy protocol, including the absence of data access restrictions on eHAC users. In addition, the impact is also quite severe, considering this is evidence of the fragility of the Indonesian government's cybersecurity system. Therefore, it is natural that we consider this incident a serious violation, or in other words, this is a serious matter to be addressed immediately (European Parliament, 2015).

Based on the explanation above, it is hypothesized that an accurate repressive measure is needed to deal with cases of personal data leakage. This repressive measure can be realized by applying criminal liability or withdrawing the settlement of personal data leakage cases to the realm of criminal law. However, it must be noted that here the criminal law is only applied as an ultimum remidium. Criminal law aims to prevent harm, embedded in communicating the wrongfulness and moral blame of the conduct that the crimes proscribe (Green, 2004). The moral directions that criminal law gives us humans somewhat require the potential offender to be morally attributable and deterred by the threat of penal sanctions (Hessick, 2006).

In short, criminal law can be applied to perpetrators of leaking personal data. However, it is necessary to identify which actor fulfills causality as the cause of the data leak. This is important to take into account because it could be a blurring of accountability. An example is whether application/platform programmers can be subject to criminal liability in the event of a data leak? Or is it the user or the party who runs/controls the program that should be responsible?

One of the criminal liability models that can be used to solve the above problems is The Natural-Probable-Consequence Liability Model. This model assumes deep involvement of the programmers and users but without any intention of committing data leaking. This model is based upon the ability of the programmers to foresee potential offenses. In other words, programmers and users cannot predict adequate risk management and do not apply the concept of due diligence. Programmers' and users' behavior can be categorized as unconscious culpability, namely negligentia. Programmers and users have no idea about the consequences of his carelessness. In this case, programmers and users do not have any thoughts about the possible effects that will arise.

The above concept can be said to be by the arrangement in Art. 82 GDPR stipulates that "Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or Contrary to lawful instructions of the controller. The essence of the rule is that the controller, in this case, it can be told that the programmer or user can be held responsible, even pay compensation to the injured party. So, with this concept, the program maker and/or the party running/controlling the program should be subject to criminal liability.

Finally, regarding which regulations can be applied, several articles in the ITE Law can be used (Makarim, 2020). Data leaks can generally occur due to intrusion from outside (illegal access) into the system or outside the system (interception or man in the middle attack). However, leakage may also occur from the act of leaking from an insider who sends the data outside the system, where the insider should maintain the confidentiality of the user's data. As the controller and data processor, the corporation must be responsible for the security system both physically and logically. Therefore, at least the act of theft or leakage can optimize the provisions of articles 30 and 32 of the ITE Law regarding illegal access and data interference.

In addition, Edmon Makarim continued that criminal responsibility should also not release the custodian, including the organizers of darknet sites that become black-market (Makarim, 2020). Offering personal data obtained illegally is like trading stolen goods on the black market as regulated in article 480 of the Criminal Code. Furthermore, apart from the main actors, of course, there are accompaniment actions that must be pursued by law enforcers, such as corporations and agencies that intentionally do not own and maintain their electronic security systems for proper management of personal data. It should also be said to be responsible for providing the means to commit crimes to the public. Furthermore, in article 65 paragraph (2) of the Trade Law, there is also a provision for the corporate crime if PMSE conducts a trade that is not following what it has stated.

Future policy

The common thread between personal data protection and the implementation of SPBE is related to how the State or government uses data regarding the people it owns, considering that data and information are essential elements in SPBE. It should be noted together, although personal data is an issue that is often discussed internationally until now there is no Model Law that can be referred to or become a guideline.

Furthermore, taking into account the current developments, the legal product that is closest to being called a Model Law is the GDPR which has been in effect since 2018. Referring to the GDPR, at least there are main points as prerequisites for the protection of privacy and personal data, including:

a. Requiring the consent of subjects for data processing
b. Anonymizing collected data to protect privacy
c. Providing data breach notifications
d. Safely handling the transfer of data across borders
e. Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

For this reason, it is necessary to ensure that future regulations/policies must meet some of the requirements above, or at least contain regulations related to some of the main requirements above.

In addition, in addition to the substance of the regulation that can reflect on the GDPR, it is necessary to have another police law that can support personal data protection policies in general. Based on the various previous explanations, at least there are legal steps that can be taken to increase efforts to protect personal data in Indonesia. First, the Personal Data Protection Bill should be pushed to be passed soon. Currently, the Personal Data Protection Bill is one of the bills

that has entered the discussion stage. A law that specifically regulates the protection of personal data can minimize and eliminate regulatory gaps that exist in various existing laws. In addition, it is undeniable that in the end, a system or technology that is built must comply with the legal provisions in force in a country.

Second, is the application of the principles of Data Protection by Design and by Default. This principle adopts the previously existing Privacy by Design principles. In Article 25(2) Regulation (EU) 2016/679 GDPR, Data Protection by Design is intended that the organization or agency, from the earliest stage of designing data processing and at the time the processing is carried out, must implement appropriate technical and organizational measures to be able to integrate the necessary safeguards in data processing to meet the regulated requirements and protect the rights of data subjects. Meanwhile, based on Article 1 point 6 Regulation of the Minister of Communication and Information Technology Number 4 of 2016 concerning Management Systems Information Security, Data Protection by Default means that organizations or agencies must ensure that personal data is processed with the highest privacy protection. By default, personal data can only be accessed for a specific purpose and cannot be accessed by just anyone.103 However, an important point that also needs to be accommodated is that the regulation regarding the rights of data subjects must also be clarified.

Third, improve data security standards and implementation of information security. When referring to the applicable provisions, the technical rules regarding information security can be found in Permenkominfo No. 4 of 2016 concerning the Information Security Management System. Information security itself is defined as the maintenance of confidentiality, integrity, and availability of information.104 In this aspect, what undoubtedly needs to be considered is to ensure that government agencies and the State implement information security standards in the processing of people's data.

Conclusion

There are two conclusions drawn based on the whole discussion above. First, the concept of liability in cases of personal data leakage in principle can be subject to administrative sanctions. This concept is because there is an element of abuse of authority by government officials, which results in the leakage of public personal data. On the other hand, in the concept of criminal liability, programmers or users can be held accountable, even paying compensation to the injured party.

Second, in the concept of policy, it is necessary to pay attention to the balance between the community's interests and the government. On the one hand, the public has an interest in the privacy and security of personal data held by government agencies or the State so that it is not misused. The State, on the other hand, needs to use people's data to improve the administration and public services provided to meet the needs of the community. In addition, considering the current regulatory conditions, it is essential to have a separate law as a solid basis to protect personal data. Last but not least is the need to ensure that all government and state agencies implement and improve security standards for data and information held to minimize the impact of cyber threats or attacks on data and information

References

Chandra, G. N. (2021). *Gov't launches investigation after data of 1.3m reportedly leaked from its covid-19 tracking app*. https://jakartaglobe.id/tech/govt-launches-investigation-after-data-of-13m-reportedly-leaked-from-its-covid19-tracking-app. Accessed: 10 November 2021

European Parliament. (2015). E-*Government: Using technology to improve public services and democratic participations*. European Union.

Green, S. (2004). *Moral ambiguity in white collar criminal law*. Notre Dame journal of law, ethics & public policy 18

Heesick, C. B. (2006). Motive's role in criminal punishment. *Southern California law review, 80*(1), 1-5.

Makarim, E. (2020). *Legal liability regarding personal data leakage*. https://law.ui.ac.id/v3/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh-edmon-makarim/, 20 September 2021