Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (1337-1354)

Legal Certainty: Is There Really Such a Thing as Indonesian Banking Personal Data Regulation?

Kartika Sasi Wahyuningrum[1], Hafrida[2], & Elly Sudarti[3]

Abstract

The objective of this research is to examine the regulation of criminal liability for banking personal data in Indonesia, which currently lacks a coherent framework. The aim of this paper is to examine the regulation of personal data control in Indonesia in general and the specific regulation of banking-related personal data in accordance with the principles of Indonesian criminal law. The findings of this study can be summarised as follows. Firstly, the concept of liability and protection of personal data in general regulates acts, liability and criminal sanctions that are addressed to the legal subject 'person' and not legal entities. Secondly, the author provides the concept of liability and protection of criminal law regarding banking personal data in Indonesia, which regulates the legal subject 'legal entity' and can be given types of criminal acts, criminal liability and criminal sanctions using a double track system.

Keywords: Legal Certainty, Personal Data, Banking.

Introduction

The objective of this research is to examine the regulatory framework governing criminal liability for the misuse of banking personal data in Indonesia. In the context of criminal liability for personal data in the modern era, this criminal act can be classified as a *Mayantara* crime. The primary objective of this research is to examine the potential criminal liability of banks as legal entities with regard to their customers' personal data. One of the *Mayantara* crimes that frequently occurs in the context of banking personal data is the hacking of personal data.

In the view of Agus Triono, hacking represents an act perpetrated by an individual or collective of individuals with the intention of illegally accessing, modifying, or retrieving electronic data belonging to another person without the requisite authorisation or legal entitlement (Agus Triono, 2023). The objective of this hacking is typically to perpetrate a range of criminal activities, including fraud, data interception, hacking, email spamming, and the manipulation of data belonging to others. These actions can result in significant financial and non-financial losses (Firdaus, 2023).

Intermediary crimes, such as those perpetrated by hackers, are a common occurrence in Indonesia (Sulisrudatin, 2018). It is therefore incumbent upon banks to safeguard personal data. The term "data protection" is essentially synonymous with "privacy," as initially defined by Allan Westin. Westin's definition of privacy is the right of individuals, groups, or institutions to determine whether or not information about them will be communicated to other parties. This definition is commonly referred to as "information privacy," as it pertains specifically to

[1] Faculty of Law, IBA University. Emil: Kartikasasi989@gmail.com
[2] Faculty of Law, Jambi University. Email: hafrida_hukum@unja.ac.id
[3] Faculty of Law, Jambi University. Email: Elly_sudarti@unja.ac.id

personal information. Furthermore, data protection is a fundamental human right. Indeed, a number of countries have recognised data protection as a constitutional right or in the form of 'data habeas', which is the right of an individual to obtain security for their data and to be justified when errors are found against their data. A number of countries with diverse histories and cultures, including Albania, Armenia, the Philippines, Timor-Leste, Colombia and Argentina, have recognised the role that data protection can play in facilitating democratic processes and have enshrined its protection in their constitutions (Greenleaf, 2012).

It is the responsibility of the bank to safeguard the personal data of its customers. However, despite the existence of Law 7 of 1992 concerning banking (Banking Law), there is a lack of specific regulation concerning the protection and criminal liability of personal data in the context of banking in Indonesia.

The protection of personal data is only explicitly addressed in Law 1 of 2024, which concerns amendments to Law Number 19 of 2016, which in turn concerns amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

Despite the fact that Indonesia has established regulations governing the protection of personal data in general, the Banking Law is nevertheless required to regulate the protection and criminal liability of personal data that is specific to the banking sector. In the view of the author, it is not possible for the Banking Law to be regarded as a special arrangement that is subject to or follows the criminal elements of the ITE and PDP Laws, as it is not *lex specialis.*

The principle of *lex specialis derogat legi generali*, which may be translated as 'more specific regulations override more general regulations', is a fundamental tenet of legal theory. The principle of lex specialis derogat legi generali is applicable only to two regulations that are hierarchically equal and regulate the same material. Conversely, the Banking Law does not contain any provisions pertaining to the criminal liability of personal data.

Methods

The research method employed in this study is the normative juridical method. This research involves examining primary legal materials, including statutory regulations governing personal data protection in Indonesia's banking sector, such as Law No. 27 of 2022 on Personal Data Protection and related sectoral regulations. Additionally, secondary legal materials, such as documents, journals, and relevant literature, are analyzed to provide a comprehensive perspective on the existing legal certainty. A conceptual approach is utilized to explore relevant legal theories in understanding legal certainty and its implications for personal data protection within Indonesia's banking system. The analysis is conducted descriptively and qualitatively to identify weaknesses and regulatory gaps affecting the practical implementation of these provisions.

Disscussion

A. Liability Arrangements and Personal Data Protection in Indonesia

The objective of this discussion is to examine the liability and protection of personal data in Indonesia. To this end, we will undertake a dogmatic examination of the existing arrangements related to personal data. In the context of the offence of hacking personal data, it is evident that the Indonesian people have acknowledged the role of the Criminal Code (KUHP) as the foundation for the criminal offence regulations that govern the Indonesian legal system. However, the existence of legal norms that accommodate the increasingly developing information and technology sector has not been aligned with this evolution, and still creates a legal vacuum. The issue of criminality in the digital domain has started to be addressed with the introduction of the provisions set forth in Law Number 11 of 2008, as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law). Accordingly, the ITE Law provides the following regulations pertaining to the protection and liability of personal data:

1. Law Number 11 Year 2008 as amended by Law Number 19 Year 2016 on Electronic Information and Transactions (or hereinafter referred to as ITE Law).

In general, the ITE Law has regulated the prohibition of the criminal offence of hacking, as well as divided the criminal offence of hacking into several articles, which are as follows:

Article 30 of ITE Law

1) Any individual who intentionally and without authorization gains access to another person's computer and/or electronic system by any means is considered to have committed the offense of computer and/or electronic system intrusion.
2) Any individual who intentionally and without authorization accesses a computer and/or electronic system by any means with the intention of obtaining electronic information and/or electronic documents.
3) Any individual who gains access to a computer and/or electronic system by any means, including by breaching, breaking through, exceeding, or penetrating a security system, is considered to have committed the offence of unauthorised access.

Article 31 of ITE Law

1) Any individual who intentionally and without right or unlawfully intercepts or taps electronic information and/or electronic documents in a computer and/or certain electronic system belonging to another person.
2) Any individual shall intentionally and without right or unlawfully intercept the transmission of electronic information and/or electronic documents that are not public from, to, and within a certain computer and/or electronic system belonging to another individual. This shall be done either without causing any change or without causing any change, omission, and/or termination of the electronic information and/or electronic documents being transmitted.
3) The provisions set forth in paragraphs (1) and (2) shall not apply to interception or wiretapping conducted in the context of law enforcement at the request of the

police, prosecutor's office, or other institutions whose authority is stipulated by law.

4) Further provisions regarding the interception procedures as referred to in paragraph (3) shall be established by legislative decree.

Article 32 of ITE Law

1) Any individual who intentionally and without right or unlawfully alters, adds, subtracts, transmits, damages, removes, moves, or conceals any electronic information and/or electronic documents belonging to another individual or to the public is in violation of this policy.
2) Any individual who intentionally and without right or unlawfully transfers or relocates electronic information and/or electronic documents to the electronic system of another individual who is not entitled to do so.
3) In instances where the aforementioned acts result in the disclosure of confidential electronic information and/or electronic documents to the public, the data integrity is compromised.

In light of the wording of Articles 30, 31 and 32 of the ITE Law, it becomes evident that the subjective element, namely the error in the formulation of the act of data hacking, is comparable, namely 'Every Person intentionally and without rights'. Consequently, it can be stated that the subjective element is intentional (*Dolus*) and not *culpa*. Furthermore, the element of intentionality is characterised by a lack of external pressure and the absence of compelling circumstances caused by humans (*Overmacht*), and compelling circumstances that arise are not the result of humans (*noodtoestand*). In addition, the purpose of obtaining electronic information and/or electronic documents represents a further subjective element.

In discussing the subjective elements in the formulation of criminal offences according to Lamintang, it can be seen that these elements are attached to the perpetrator or related to the perpetrator. In other words, they are included in the perpetrator's heart. The subjective elements of a criminal offence are as follows:

1. Intentional (*Dolus)* or Unintentional (*Culpa*);
2. Intent or *Voornemen* on an Attempt or *Poging*; 3.
3. Various Intentions or *Oogmerk*, such as those found in the crimes of theft, fraud, extortion, forgery, and others;
4. Premeditation or *Voorbedachte Raad*, as found in the crime of premeditated murder; 4.
5. Fear or *Vrees*.

The acts described in Articles 30-32 of the ITE Law are defined as "premeditated intentions" (*voorbedachte raad*) in Dutch criminal law. This raises the question of why such a definition is used. An examination of the process of hacking reveals that it is not necessarily carried out spontaneously due to the convergence of opportunities and intentions. In contrast to conventional criminal acts, which can be perpetrated due to the convergence of opportunity and intention, the commission of cybercrime necessitates a more meticulous and deliberate planning process, including the creation of opportunities. In carrying out hacking actions, a hacker will typically employ one of two methods, as outlined by David Wall:

1. The act of gaining access to a system or area without the consent of the authorised individual or entity. A computer or electronic system may be subject to hacking as a result of inherent vulnerabilities or external attacks that compromise the integrity of operational systems and/or software. The aforementioned weaknesses in operational systems and software permit the perpetrators to gain access without authorised consent (David S. Wall, 2015).
2. The act of perpetrating a criminal act subsequent to gaining access to a location without the requisite authorisation. Once unauthorised access has been gained, the perpetrator proceeds to commit the crime. The objective of the criminal act of hacking is the acquisition of data and/or access to computers. Consequently, criminal acts of hacking frequently result in the theft, manipulation, or sabotage of data. According to Roderick, S. Graham, a person is said to commit a criminal offence of hacking or hacking after having committed a criminal offence of hacking if, having gained access without official approval, the perpetrator then proceeds to commit a crime (RS & K, 2019).

In light of the aforementioned explanation, it can be concluded that the subjective element, namely 'intentional' wrongdoing based on Articles 30 to 32 of the ITE Law, is not a mistake without prior planning and is also not a case of coercion or external force. Consequently, data hacking constitutes a grave criminal offence, as it has the potential to result in substantial material and immaterial losses. In this context, the term "intent" denotes a conscious and deliberate act in violation of established legal norms. In relation to the concept of 'without right', the judge presiding over the case, as outlined in Decision No. 45/Pid.B/2012/PN.MSH, elucidated that the term 'without right' does not imply a lack of entitlement or permission from an authorised party. The term 'against the law' is open to interpretation. One such interpretation is that proposed by the Hof van Cassatie, which uses the term *'Zonder Eigenrecht'* (without rights) (Khalisah & Kirana, 2022).

The element under consideration is that of "actors who access without authorised consent." The ITE Law elucidates the concept of access. In the context of information technology, access can be defined as an activity that interacts with electronic systems, whether standalone or within a network. In the meantime, electronic systems are defined as electronic devices and procedures utilised in the context of electronic information. In other words, activities that constitute access include interactions or relationships with electronic systems or networks that can be used to display, collect, store, and disseminate information. As previously stated, the criminal offence of hacking is divided into two stages: firstly, gaining access without official approval; and secondly, the perpetrator committing a crime.

In addition to subjective elements, the formulation of criminal offences must also comply with objective criteria. The following section will provide an explanation of the provisions set forth in Articles 30-32 of the ITE Law.

In accordance with Article 30 of the ITE Law, the object element is defined as follows:

- In paragraph 1, the term denotes the act of unlawfully accessing another person's computer and/or electronic system by any means.

- Paragraph 2 provides an additional clarification that the act is undertaken with the specific intention of obtaining electronic information and/or electronic documents.
- In addition to the aforementioned means of confirmation, as outlined in Paragraph 1, namely: by violating, breaching, exceeding, or circumventing the security system, Paragraph 3 stipulates that the act in question must be carried out by any means.

In accordance with Article 31 of the ITE Law, which is an objective element, namely:

- In accordance with the legislation in question, the interception or wiretapping of electronic information and/or electronic documents within a specific computer and/or electronic system belonging to another individual is prohibited.
- In paragraph 2, two types of acts are delineated. The first act is defined as "to intercept the transmission of electronic information and/or electronic documents that are not public, from, to, and within a certain computer and/or electronic system belonging to another person." The second act, either of which does not result in any change or causes the change, removal, and/or termination of electronic information and/or electronic documents that are being transmitted. This Horse Act underscores the ramifications of the initial act, thus necessitating the application of the theory of causality.
- Paragraph 3 elucidates that the criminal offenses delineated in paragraphs 1 and 2 are not subject to enforcement if they are conducted within the context of law enforcement at the behest of the police, prosecutor's office, or other institutions whose authority is determined by law. Consequently, paragraph 3 presents justification as a means of eliminating criminal offences. This justification, therefore, removes the unlawfulness of the act, despite the fact that the act has fulfilled the criteria set out in the legislation. In the absence of unlawful conduct, there can be no basis for imposing a penalty. This is due to the fact that, in paragraph 3, the criminal act is defined as a duty and an official order.

In accordance with Article 32 of the ITE Law, the objective elements delineated in the following articles are as follows:

- In paragraph 1, the acts described are in contravention of the law, specifically in relation to the alteration, addition, reduction, transmission, damage, elimination, movement and concealment of electronic information and/or electronic documents belonging to other individuals or public property.
- In paragraph 2, the act committed is described as the movement or transfer of electronic information and/or electronic documents to the electronic system of another person who is not entitled. Additionally, this paragraph states that other perpetrators are involved in data hacking, as it is known to move/transfer electronic documents to other people without rights. Therefore, it can be concluded that data hacking is both an individual and organised crime.
- In paragraph 3, the perpetrators' actions result in the public access to electronic documents that are confidential.

Thus, the criminal offence of hacking in the ITE Law in three articles, namely Article 30, Article 31, and Article 32. Article 30 paragraph (2) and Article 30

paragraph (3) of the ITE Law are *lex specialis* of Article 30 paragraph (1). Meanwhile, Article 31 and Article 32 of the ITE Law are other forms of Article 30.

1. Law Number 27 Year 2022 on Personal Data Protection

The UU PDP has established a comprehensive regulatory framework, encompassing definitions and criminal sanctions, with the objective of safeguarding personal data in Indonesia. The definition of personal data as set forth in UU PDP is delineated in the general provisions of Article 1, number 1, which states:

"The term "personal data" is defined as any information about an identifiable individual, whether directly or indirectly obtained through electronic or non-electronic systems.

In accordance with the stipulations set forth in Article 1, Section 1, the data in question is not merely an individual (natuurlijk persoon), but also a person or legal entity (recht persoon). The data may be identified and distinguished from other data sets. The prohibited acts set forth in the PDP Law are also addressed in Chapter XIII, Articles 65 and 66.

Article 65 of PDP Law

1) It is hereby prohibited for any individual to unlawfully obtain or collect personal data that does not belong to them with the intention of benefiting themselves or another person, which may result in harm to the data subject.
2) Any individual shall be prohibited from unlawfully disclosing personal data that does not belong to them.
3) Any individual shall be prohibited from unlawfully utilising personal data that does not belong to them.

The provisions set forth in Article 65, paragraphs (1), (2), and (3), represent an illicit collection of personal data belonging to another individual (without consent and/or not in accordance with legal and regulatory frameworks), dissemination of personal data that does not rightfully belong to them, and utilization of personal data that does not rightfully belong to them. This rule serves as a legal foundation for filing a tort lawsuit in the event of a personal data breach.

In order to ascertain the subjective and objective elements of the aforementioned offences, it is necessary to conduct an analysis of the contents of Articles 65 and 66 of the PDP Law.

The subjective elements of Article 65 of the PDP Law are as follows:

a. With the intention of benefiting oneself
b. With the intention of benefiting another person
c. With the purpose of disclosing personal data
d. With the purpose of using personal data that does not belong to him/her

The Objective Elements in Article 65 are as follows:

- It is prohibited for any individual to engage in any unlawful activities.
- It is prohibited to obtain or collect personal data that does not belong to the individual in question.
- Such actions may ultimately result in harm to the data subject.

Article 66 of the PDP Law

"It is prohibited for any individual to create or alter personal data with the intention of benefiting themselves or others, and with the understanding that such actions may result in harm to others."

In light of the aforementioned explanation of Article 66 of the PDP Law, it becomes evident that the formulation of criminal acts cannot be dissociated from the objective and subjective elements that constitute it. The subjective elements set forth in Article 66 of the PDP Law are as follows:

a. With the deliberate intention of benefiting oneself and others through the use of illicit methods.
b. With the intention of benefiting oneself.
c. With the intention of benefiting another individual.

The Objective Elements in Article 66 of the PDP Law are as follows:

a. Every Person is prohibited from creating false Personal Data
b. falsify Personal Data
c. causing harm to others.

The illicit acquisition and disclosure of personal data is explicitly proscribed in both the ITE Law and the PDP Law. Meanwhile, the Banking Law and the Consumer Protection Law merely set forth protections, and do not address the issue of personal hacking in the context of banking transactions between financial institutions and their customers. It is imperative that a legislative act be enacted to define and criminalize the act of hacking into banking personal data.

A. The Concept of Liability and Criminal Protection of Personal Data in Banking

In discussing the concept of personal data criminal liability and protection, it is necessary to consider three fundamental problems in criminal law: criminal acts, criminal responsibility and criminal sanctions (Yuniarti, 2019). Accordingly, the author will formulate the Personal Data Liability and Criminal Protection legislation in accordance with the principles of legal positivism.

The following article discusses three principal issues pertaining to the definition of a criminal offence. One of the criminal law experts, Simons, defined a criminal offence (*strafbaar feit*) as 'an action that is punishable by law, which is wrongful and which involves a person who is capable of being held responsible'. This definition comprises the following elements: The second element is human action, which may be either positive or negative. This encompasses actions such as doing, not doing, or allowing. The individual in question is threatened with punishment. In contravention of the law (*onrechmatige daad*); Committed with fault (*met schuld in verband staand*). In the context of criminal law, the term "person" refers to an individual who is capable of bearing responsibility for their actions) (Guswandri et al., 2023).

In formulating the main crime, Simon posits that the act of the legal subject must be constrained by limits on the types of criminal acts related to liability and the protection of personal data. To what extent are banks required to account for and protect personal data? What constitutes personal data?

The delineation of what constitutes personal information and what does not constitute personal information was proposed by Jerry Kang. Information is

classified as personal if it can be used to identify an individual through three distinct means. This may be demonstrated by:

1) a relationship of *authorship* with the individual;
2) describing permanent individual characteristics; or information that can be used as an instrument to describe an individual (Kang, 2006).

From a philosophical perspective, efforts to regulate the right to privacy of personal data represent a manifestation of the recognition and protection of fundamental human rights. In light of the aforementioned considerations, the drafting of the Personal Data Protection Bill is firmly anchored in a robust and accountable philosophical framework. The philosophical foundation is Pancasila, which can be defined as a legal ideal or construction of thought that serves to direct the law towards a desired outcome.

In light of the restrictions on the processing of personal data as set forth by Jerry Kang, the provisions of the banking law pertaining to liability and the protection of personal data may be informed by these limitations. It is imperative that criminal acts be formulated in accordance with the provisions that define the essential elements of criminal offenses. The following paragraphs provide an explanation of the three elements in question: the element of action, the element of responsibility and the element of sanction.

1. The concept of criminal offences in banking laws regarding liability and personal data protection.

In essence, an act can be defined as criminal if it meets the criteria set forth by objective and subjective elements. In the view of Lamintang, the objective elements of an act are those pertaining to circumstances, namely the circumstances in which the actions of the perpetrator must be carried out (P. A. F. Lamintang, 2013).

In addition, S. R. Sianturi posits that the objective element of a criminal act must necessarily encompass both formal and material elements. The formal element pertains to the act's conformity with the specific formulation or wording of the law (t*atbestandsmaszigkeit)*, whereas the material element concerns the act's intrinsic nature as being contrary to the ideals of community association or in contravention of the law (*rechtswidigkeit*). Furthermore, Sianturi elucidated that the objective element pertains to the act's illegality, its status as either prohibited or required by law, and its punishability. Additionally, the act must be committed at a specific time, place, and condition (S. R. Sianturi, 2002).

In the context of criminal law, the subjective element refers to the mental state of the perpetrator at the time of the offence. This encompasses not only the perpetrator's intentions and knowledge, but also their emotions, beliefs, and attitudes. In other words, the subjective element encompasses everything that is in the perpetrator's heart.

In accordance with the delineation of objective and subjective elements, criminal acts must also be classified according to the typology of offences. In his treatise, Principles of Criminal Law, Andi Hamzah identifies the following categories of offences:

1. **Criminal offences and *misdemeanours (misdrijven enoventredingen)*** Criminal offences frequently encompass actions that are perceived as antisocial conduct by the general public. Conversely, misdemeanours are defined as criminal acts that are specifically delineated by legislation.
2. **Materil and Formil *Delicts (materiele end formele delicten***

A material offence is defined as an offence where, in addition to the prohibited act being committed, there must still be a consequence arising from the act. This is in contrast to a formal offence, where the act itself is sufficient to constitute the offence. In order for a criminal offence to be considered complete, it must be a material offence. This is demonstrated in Article 187 of the Criminal Code on arson and Article 338 of the Criminal Code on murder. In contrast, a formal offence is defined as a prohibited act (along with other relevant circumstances) without consideration of the resulting consequences. This is exemplified by Articles 160, 209, 242, 263, and 362 of the Criminal Code.

3. **Delict Komisi dan Delict Omisi (*commission offences and omission offences)***

A delict of commission (*delicta commissionis*) is defined as an offence committed by an act. In contrast, omission offences (*ommissiedelicten*) are committed by failing to act or to take notice (*nalaten*). Omission offences are divided into two categories.

- A pure omission offence is one that involves the failure to act in accordance with a legal obligation, as set forth in Articles 164, 224, 522, and 511 of the Criminal Code.
- Impure omissions (delicto commissionis per omissionem) constitute a breach of the law when the consequence of an action is not intended, despite the potential for such a consequence to be caused by an omission. For example, Article 338 of the Criminal Code pertains to the offence of murder by omission, whereby the failure to provide sustenance results in the death of the victim.

4. **Completed and continuing offences (*af lopende en voordorende delicten)***

A completed offence is defined as an offence that has been perpetrated through the commission of one or more specific acts. A continuing offence is defined as an offence that occurs due to the continuation of the circumstances that are prohibited by law.

5. **Single and concurrent offences (*enkelvoudige en samengesteededelicten***

A serial offence is defined as an offence that is committed through a series of acts, rather than a single act. Van Hamel refers to this as a collective offence. The most illustrative examples are those offences committed as a matter of habit, as exemplified by Article 296 of the Criminal Code.

6. **Deliberate Offences and Offences of Negligence or Culpa (*doleuse en culpose dellicten*)**

Deliberate offences and negligent offences are important in terms of attempt, participation, imprisonment and forfeiture.

7. **Delict Propria and Delict Komun (delicta propria en commune delicten)**

The term "*delik propia"* is used to describe criminal acts that can only be perpetrated by individuals who possess specific characteristics or qualifications. These include offences related to one's professional or military status, as well as

other similar offences. In contrast, offences committed by society in general are referred to as communal offences.

8. **Complaint offences and general offences**,

A complaint offence is defined as an offence that can be prosecuted on the basis of a formal complaint from an aggrieved person. In other words, the absence of a complaint precludes the possibility of prosecuting the offence. In contrast, a general offence is one that can be prosecuted without the necessity of a complaint.

9. **Based on nature, it has two characteristics:**(Van Hammel, 2003)

a. In this criminal offence, the act in question is prohibited and punishable by law from the moment of its completion.

b. In this type of criminal offence, the occurrence of an effect is prohibited and punishable by law from the moment of its occurrence.

In light of the aforementioned explanation, the author posits that the act of hacking banking personal data can be conceptualised as a criminal act. The question thus arises as to why a crime is not regarded as an offence. The classification of an act as either a crime or an offence determines the severity and degree of criminal sanctions imposed. In his book entitled Principles of Criminal Law, Moelyatno states that...

The distinction between crimes and offences in Indonesian criminal law is based solely on the severity and leniency of the associated criminal sanctions. There are, however, other differences.

1. Imprisonment is a sentence that is imposed exclusively for criminal offences.
2. In the context of criminal proceedings, the form of guilt (wilfulness or negligence) required to prove an offence is the responsibility of the Prosecutor. In contrast, in the context of civil or administrative offences, this is not a necessary element of proof. In this regard, crimes are also differentiated into those of dolus and those of culpa.
3. Attempting to commit an offence is not a punishable act (Article 54). Furthermore, assistance in the commission of an offence is not a punishable act (Article 60).
4. The period of eligibility for both the determination and execution of punishment for an offence is shorter than for a crime by one year and two years, respectively.
5. In the event of concurrence (concursus), the punishments are different for offences and crimes. The cumulation of light punishments is easier than that of heavy punishments (Moelyatno, 1993).

The subsequent category within the classification of criminal acts of hacking personal banking data is that of a complaint offence, which is a formal offence. The question thus arises as to why this particular act is classified as a complaint offence. This is due to the fact that the act of data hacking is a criminal offence that focuses on the victim's suffering. Consequently, the aggrieved party is a specific victim, particularly in cases involving personal data. Furthermore, it is necessary to define this as a formal offence, as this implies that the act in question is prohibited, and that the consequences of the action must be questioned. Therefore, even if there has been no material or immaterial loss, the act of hacking can be categorised as a criminal act. In order to ensure legal certainty and justice.

2. Concept of Criminal Liability in Banking Law regarding liability and protection of personal data.

n accordance with Simons strafbaarfeit, criminal responsibility entails the performance of an act by a person who is capable of being held accountable and who has committed an act that is contrary to the law (Aryo Fadlian, 2020).

Michael McGrath and Brent Turvey, "a *Criminal responsibility evaluations deal with the mental state of an offender at the time of a crime. They were referred to as Insanity Pleas in the past. This evaluation should not be done by a treating behavioral health provider. It is not unheard of for a practitioner in a jail setting to evaluate for treatment, competency to stand trial and criminal responsibility at the same time. Such situations belie ignorance of both ethical concerns and lack of formal forensic training. Treating someone is so fundamentally different from assessing criminal responsibility that a practitioner ought to refuse to participate in such a situation"* (McGrath & Turvey, 2021)*"*

It can be concluded that mental health is of great consequence with regard to the responsibility of individuals in legal matters. It is imperative that mental health is not used as a pretext for corporations to evade criminal liability.

In the context of criminal liability, Sudarto posits that the mere act of committing an act that is contrary to or against the law is insufficient grounds for criminalisation. Therefore, despite the act meeting the second formulation of the law and being unjustified (an objective breach of a penal provision), Nevertheless, this does not satisfy the criterion for the imposition of punishment. In order for punishment to be imposed, it is necessary that the individual who has committed the act be found to have acted with guilt or be guilty of the offence (subjective guilt). In other words, accountability for actions can only be determined from the perspective of the actions themselves. The act can only be held accountable to the person.

Moreover, Sudarto posited that the principle of "no punishment without fault" (keine Strafe ohne Schuld, geen straf zonder schuld, or nulla poena sine culpa) is applicable. In this context, the term "culpa" is employed in a comprehensive manner, encompassing both intention and knowledge. The term "culpability" is used to describe the mental state of the individual who has committed an act, and the act itself is considered blameworthy (Sudarto, 1988).

Roesin Saleh menyatakan, seseorang memiliki kesalahan apabila pada saat melakukan tindak pidana dari sudut pandang masyarakat, ia dapat dicela untuk itu. Karena dianggap dapat berbuat lain, jika ia tidak mau berbuat demikian, lanjut Saleh:

Roeslan Dari segi masyarakat, 'hal ini menunjukkan pandangan normatif tentang kesalahan. Seperti diketahui, masyarakat memiliki pandangan yang bersifat *psikologis* tentang rasa bersalah. Ini adalah, misalnya, pandangan para perumus W.v.S. Tetapi kemudian pandangan ini ditinggalkan, dan orang mengambil pandangan normatif. Ada atau tidaknya kesalahan tidak ditentukan oleh keadaan pikiran terdakwa, tetapi tergantung pada bagaimana hukum menilai keadaan pikirannya, apakah terpenuhi atau tidak ada kesalahan (Roeslan saleh, 1993).

A closer examination of the definition of guilt according to several criminal law experts reveals a diversity of perspectives.

In his explanation of schuldbegrip, Jonkers divides the definition of fault into three parts, namely:

a. Other than wilfulness or negligence (*apzet of schuld*).

b. It also includes unlawfulness (*de wederrechtelijkheid*).

c. Ability*to* be responsible (*de toerekenbaarheid*).

Pompe posits that the concept of fault is inherently reprehensible (verwijtbaarheid) and, in and of itself, is an insufficient deterrent to unlawful conduct (der wederrechtelijke gedraging).

In contrast, the concept of corporate responsibility differs from that of personal responsibility. Herlina Manullarng posits that criminal responsibility can be attributed not only to individuals, but also to corporations, which are themselves legal subjects. The concept of corporate liability is formulated differently from Simon's. The question of corporate guilt is determined by an examination of whether the actions of the management, acting on behalf of and in the interests of the corporation, can be considered culpable. If the answer is affirmative, the corporation is deemed culpable for the criminal act in question, and the converse is also true (Manullarng & Pasaribu, 2020).

In the context of legal entities (rechtspersoon) as legal subjects, Sudikno Mertokusumo posited that:

It is a fallacy to assume that only humans can be subjects of law. In order for a subject to exist, it is necessary for something other than a human being to become a subject of law. In addition to humans, there are also recognised legal subjects, namely legal entities. A legal entity is defined as an organisation or group of people that has been granted certain rights and obligations by virtue of its status as a legal subject. The state and limited liability companies, for example, are constituted as legal entities, comprising organisations or groups of people. A legal entity functions as a unified entity within the legal system, analogous to an individual. The law establishes legal entities because the acknowledgement of organisations or groups of people as subjects of law is highly advantageous, facilitating the smooth functioning of legal processes." (Sudikno Mertokusumo, 1988)

Furthermore, according to H. Riduan Syahrani I

In the context of legal terminology, the term "legal entity" (or "rechtspersoon" in Dutch) refers to a person or entity that is recognised as a legal subject in a given jurisdiction. A legal entity that is devoid of the essential quality of a soul. As legal subjects, legal entities are also capable of entering into legal relations with other legal subjects, thereby acquiring rights and assuming obligations. It is important to note that legal entities are not permitted to engage in matters pertaining to family law, such as entering into matrimony. The sole area of legal engagement for legal entities is that of property law. This is conducted through the organs of the legal entity concerned, which are typically regulated in the articles of association and bylaws (H. Riduan Syahrani I, 2009).

R. In their publication, Legal Dictionary, Subekti and R. Tjitrosudibio posit that "legal subjects or bearers of law are humans or legal entities"(Subekti &

Tjitrosudibio, 1985). In the General Encyclopedia edited by Abdul Gafar Pringgodigdo and Hassan Shadily, the following is written:

Those who are recognised as such and who are thus able to engage in legal relationships are designated as legal subjects. In the context of Western law, the term "legal subject" is understood to refer to all human beings, with the exception of those in a state of slavery. In addition to the legal subject in the form of a natural person, there is a legal subject in the form of a human group unit called a legal entity. Examples of such entities include limited liability companies, cooperative associations and foundations.

Dwi Wahyono posits that criminal responsibility is predicated on the following doctrine:

1)Identification Doctrine;

According to this doctrine, criminal responsibility, the principle of "mens rea" is not ruled out, where according to this doctrine the mental actions or attitudes of senior corporate officials who have a "directing mind" can be considered as corporate attitudes. This means that the mental attitude is identified as a corporation, and thus the corporation can be directly accounted for. The action or will of the director is an act. and the will of the corporation.This accountability differs from vicarious liability and strict liability, wherein this identification doctrine, the principle of "mens rea" is not ruled out, whereas, in the vicarious liability and strict liability doctrines, the principle is not required. "Mens rea", or the principle of "mens rea" does not apply absolutely.

2) The doctrine of vicarious liability;

Substitute liability is someone's responsibility without personal fault, taking responsibility for the actions of others.

3) Doctrine of Strict Liability According to the Law (strict liability)

The principle of absolute responsibility without having to prove whether or not there is an element of guilt in the perpetrator of the crime. This criminal liability is known as strict liability crimes (Dwi Wahyono, 2021).

Considering the aforementioned explanation, the author posits a conceptualisation of criminal responsibility pertaining to the hacking of banking personal data. This conceptualisation is contingent upon the question of who responsible and what conditions is are necessary for criminal responsibility. In the context of hacking into banking personal data, the question of who will be held responsible can be approached from a legal perspective. This entails distinguishing between two categories of legal subjects: individuals (natuurlijke person) and legal entities (rechts-persoon).

In relation to the legal subject, the concept of 'mens rea' is pertinent, whereby the inner attitude of the perpetrator and their capacity for responsibility are considered. The capacity for moral responsibility entails the ability to discern between actions that are morally praiseworthy and those that are morally reprehensible, that is, between actions that are in accordance with the law and those that are contrary to it. Moreover, the capacity to ascertain his volition based on an awareness of the moral implications of the act. Consequently, the formulation of criminal law responsibility is defined as 'intentionality', which denotes an act that is

contrary to the law. Meanwhile, the formulation of 'intentionality' in the context of corporate liability is distinct. The question of corporate guilt is determined by an examination of whether the actions of the management, acting on behalf of and in the interests of the corporation, can be held to be at fault.

3. The Concept of Sanctions in Banking Personal Data Hacking

The imposition of criminal sanctions must be in accordance with the objectives of the law, namely legal certainty and legal justice. It is therefore important to ensure that the imposition of sanctions is not limited to physical sanctions or sanctions in the form of looting. In the context of data breaches, the legal subject is not merely an individual, but may also be a legal entity. It is therefore inappropriate to apply physical sanctions to corporations.

In modern criminal law, Muladi argues that criminal sanctions are more oriented towards the act and the perpetrator (dáad-dáder strafrecht). This approach not only includes punishment that is oriented towards suffering, but also educational content. In the evolution of contemporary legal systems, the concept of a "double track system" has emerged, signifying a distinction between criminal sanctions and action sanctions. The evolution of this legal framework has introduced the concept of "action" (maatregel) as an alternative to the conventional main punishment, particularly imprisonment. This was due to a lack of confidence in the efficacy of imprisonment as a form of punishment or sanction. The double track system encompasses both criminal sanctions and action sanctions. The double track system does not fully utilise one of the two types of sanctions. The two-track system establishes a parity between the two types of sanctions. The fundamental principle of the double track system is the equality of criminal sanctions and action sanctions (Ramadhani et al., 2012).

Indeed, the importance of both deterrence (through criminal sanctions) and guidance (through action sanctions) is equally significant. The distinction between criminal sanctions and action sanctions. The rationale behind criminal sanctions can be traced back to the fundamental question of why punishment is necessary. In contrast, action sanctions are based on the underlying purpose of punishment. Criminal sanctions are, in fact, reactive to an act. In contrast, action sanctions are more oriented towards the perpetrators of the act in question.

Criminal sanctions place emphasis on the element of retaliation, which may be defined as the deliberate imposition of suffering on the perpetrator of the crime. The focus of criminal sanctions is on the imposition of punishment for criminal acts. The purpose of action sanctions is to serve the social good. In order for a double-track system to be effective, it is essential that both the element of defamation/suffering and the element of guidance are given equal consideration within the criminal law sanction system (Sholehuddin, 2003).

The sanction or punishment system is typically divided into two models: a one-track model, also known as a single sanction system (Single Track System), and a two-track model (Double Track System). As previously stated, the concept of punishment is thought to have originated from the classical school. The classical school adheres to a single-track model, namely a single sanction system in the form of criminal sanctions, in principle (M. Sholehudin, 2004).

This concept originated in the 18th century, when an indeterministic perspective on human free will gained prominence. This view placed emphasis on the actions of those who perpetrate crimes, leading to the emergence of criminal law of conduct (dáad-strafrech). Accordingly, the traditional system of punishment places greater emphasis on the punishment of the act itself, rather than on the individual perpetrators of the crime. The definitive sentence system places the emphasis on the punishment of the act, rather than on the perpetrator) (Rabith Madah Khulaili Harsya, 2022).

In the context of the rule of law, the determination of sanctions does not take into account factors such as the age of the perpetrator, their mental state, previous criminal history, or the specific circumstances of the act or crime in question (Ruben Achmad, 2016). It is evident that the single-track system of criminal sanctions places a particular emphasis on the element of retaliation, which is deliberately applied to those who have committed criminal acts. This is done with the intention of providing a deterrent effect.

In the nineteenth century, the modern school of criminology emerged, seeking to examine the causes of crime through the lens of natural science and to engage with offenders in a constructive and corrective manner. In contrast to the classical school, this approach is based on the view of determinism and necessitates the individualisation of punishment and resocialisation for those who have committed crimes.

Barda and Muladi posit that the objective of criminal sanctions is to serve as a deterrent for criminal behaviour. The objective of sanctions is to provide assistance to the perpetrator in order to facilitate a change in behavior (Muladi & Arief, 1992). It is evident that criminal sanctions are intended to serve as a deterrent, and therefore, it can be concluded that they are indeed a form of punishment. The objective of the sanction is twofold: firstly, to protect the community and secondly, to provide guidance to the perpetrator with a view to effecting a change in their behaviour.

Criminal sanctions are imposed on individuals who perpetrate criminal acts on behalf of or for the benefit of an organisation. These include the death penalty, life imprisonment, imprisonment and other criminal sanctions regulated in other laws that are specialised (lex specialis). The double track system model of punishment allows the judge to apply not only action sanctions, but also other forms of punishment. In his work, Incorporate Crime, Sutan Remy Sjahdeini identifies a number of different forms of action sanctions, which he categorises as follows:

a. The announcement of the judge's decision constitutes a form of action sanction, whereby the decision is conveyed through electronic or print media. The objective is to humiliate the management and/or corporation. This results in a shaming effect, whereby corporations with previously positive reputations are humiliated by the announcement of the judge's decision.
b. Corporate liquidation due to corporate dissolution. If the penalty is death, then the dissolution of the corporation is tantamount to its death. The dissolution of a corporation entails the liquidation of its assets.

c. Revocation of business licence followed by liquidation of the Corporation. The application of sanctions in the form of revocation of business licence results in the corporation's permanent cessation of business activities. Nevertheless, in the event of a debt burden to creditors, the revocation of the business licence is balanced by an order to the corporate management to liquidate the corporate assets, in order to provide legal protection.
d. Suspension of Business Licence the suspension of a business licence can also be a sanction action for corporations. This may be for the suspension of certain activities, or for all corporate activities within a certain period of time, or for a period determined by the judge, or even forever.
e. Forfeiture of corporate assets by the state may be applied to part or all of the corporation's assets, including assets used directly or indirectly in corporate criminal offences.
f. Corporate takeover by the state, This differs from asset forfeiture by the state in that, in the case of asset forfeiture of the corporation, the shareholder remains the owner of the corporation. In the event of a state takeover or seizure of a corporation, all shares held by the owner are also deemed to become the property of the state. Consequently, the state assumes control of the corporation's assets and liabilities.
g. Confiscation of Corporation During the corporate examination process, the court may issue an order for the confiscation of the corporation, followed by the appointment of temporary directors to oversee its management. The court may issue a stipulation appointing one of the state-owned enterprises (SOEs) in the relevant business sector to manage the corporation on a temporary basis until the seizure is lifted (Sjahdeini, 2017).

Conclusion

The research highlights significant gaps in Indonesia's banking regulations concerning the criminal liability for the misuse of personal data, particularly in the context of hacking incidents. While laws such as the ITE Law and the Personal Data Protection Law offer a general framework for data protection, there is a distinct lack of specific provisions addressing the responsibility of banks in safeguarding personal data and the criminal consequences of breaches in the banking sector. Although the ITE Law covers hacking-related offenses, its applicability to banking data is limited, and the Banking Law does not adequately address the criminal liability for data breaches. Therefore, the author argues for the need to amend the Banking Law to provide clearer regulations and strengthen the protection of personal data within the banking sector, in line with international standards that recognize data protection as a fundamental human right.

Reference

Agus Triono. (2023). Implementasi Peretasan Sandi Vigenere Chipher Menggunakan Bahasa Pemrograman Python. *Jurnal Jocotis -Journal Science Informatica And Robotics*, *1*(1), 2.

Aryo Fadlian. (2020). Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis. *Jurnal Hukum Positum*, *5*(2), 13.

David S. Wall. (2015). Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime*, *2*(2), 71–90.

Dwi Wahyono. (2021). The Criminal Responsibility By Corporate. *International Journal Of Law Recontruction*, *5*(1), 131.

Firdaus, I. (2023). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 24.

Greenleaf, G. (2012). Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, 115.

Guswandri, R., Din, M., & Rinaldi, Y. (2023). Corporate criminal responsibility in corruption crimes. *International Journal of Law*, *9*(1), 181.

H. Riduan Syahrani I. (2009). *Kata-Kata Kunci Mempelajari Ilmu Hukum*.

Kang, J. (2006). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, *50*(4), 1193–1293.

Khalisah, A. M., & Kirana, P. (2022). Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia. *Jurist-Diction*, *5*(6), 2126.

M. Sholehudin. (2004). *Sistem sanksi dalam hukum pidana; Ide Dasar Double Track System &Implementasinya*.

Manullarng, H., & Pasaribu, R. (2020). *Pertanggungjawaban Pidana Korporasi*.

McGrath, M., & Turvey, B. (2021). Criminal Responsibility. *Ethical Justicem*, *13*, 405.

Moelyatno. (1993). *Asas-Asas Hukum Pidana*.

Muladi, & Arief, B. N. (1992). *Teori-teori dan Kebijakan Pidana*.

P. A. F. Lamintang. (2013). *Dasar-dasar Hukum Pidana Indonesia*.

Rabith Madah Khulaili Harsya. (2022). Penetapan Sanksi Pidana Dan Tindakan Sebagai Sistem Pemidanaan Di Indonesia. *Yustisia Merdeka: Jurnal Ilmiah Hukum*, *8*(2), 58.

Ramadhani, G. S., Arief, B. N., & Purwoto. (2012). Sistem Pidana dan Tindakan "Double Track System" Dalam Hukum Pidana di Indonesia. *Diponegoro Law Review*, *1*(4), 3.

Roeslan saleh. (1993). *Perbuatan pidana dan pertanggungjawaban pidana dua pengertian dasar dalam hukum pidana*.

RS, G., & K, S. 'Shawn. (2019). *Cybercrime and Digital Deviance*.

Ruben Achmad. (2016). Hakekat Keberadaan Sanksi Pidana Dan Pemidanaan Dalam Sistem Hukum Pidana. *Jurnal Fiat Justicia*, *2*(1), 18.

S. R. Sianturi. (2002). *Asas-asas Hukum Pidana di Indonesia dan Penerapan*.

Sholehuddin. (2003). *Sistem Snaksi Dalam Hukum Pidana Ide Dasar Double Track System & Impelmentasinya*.

Sjahdeini, S. R. (2017). *Ajaran Pemidaan: Tindak Pidana Korporasi & Seluk – beluknya*.

Subekti, R., & Tjitrosudibio, R. (1985). *Kamus Hukum*.

Sudarto. (1988). *Hukum Pidana 1*.

Sudikno Mertokusumo. (1988). *Mengenal Hukum (Suatu Pengantar)*.

Sulisrudatin, N. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara*, *9*(1), 28.

Van Hammel. (2003). *Rangkaian Sari Kuliah Hukum Pidana 1*.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147–154.