International Journal of Arts and Social Science www.ijassjournal.com
ISSN: 2581-7922,
Volume 5 Issue 4, April 2022

Liability for Personal Data Leakage of *Fintech* Consumer by Islamic Economic Law Perspective

Masning Nur Azizah[1], Siti Hamidah[2], Sukarmi[3]
[1,2,3(]*Faculty of Law, Universitas Brawijaya Malang, Indonesia)*

ABSTRACT: *This research is written because of the Electronic Information and Transactions Acts (UU ITE) No. 19 of 2016 Article 26 Paragraph (1) that the use of consumer personal data must be with the consent of the data owner, in its implementation there is often the use of consumer data by third parties without the owner's consent, such as the case of the Tokopedia data leak. However, there has been no settlement or civil liability carried out by parties proven to have violated the rules. This problem can be examined from the perspective of Islamic Economic Law because the development of fintech is not only in the conventional form but also in sharia form. This study aims to determine who is responsible for the leakage of consumer data and how the form of accountability takes. This research is a normative juridical method. The results reveal if there is a data leak, the fintech company is obliged to take responsibility by being responsible for errors. Meanwhile, in Islamic Economic Law, data leakage is called Al-fi'lu Al-dharar that cause dhamân or ta'widh. Because the data leak contains an element of error, the form of responsibility is to provide ta'widh to the injured party.*

KEYWORDS:*consumer personal data leakage, fintech, responsibility*

I. INTRODUCTION

Fintech(financial technology) is a new form derived from technological updates carried out in the financial sector, which can produce software, business examples, and new products with a material impact on financial service providers. The *fintech* industry has experienced various obstacles, one of which is related to consumer data security. The problem of consumer data security that is often experienced by *fintech* companies is the leakage of consumer personal data. Leakage of consumer's personal data means that consumer's personal data can be accessed by other parties who are not concerned, or have no connection to use consumer's personal data illegally. Leakage of personal data is regulated in Law no. 19 of 2016 Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions Article 26 Paragraph (1) which is referred to as the ITE Law, reads: "Unless stipulated otherwise by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the approval of the person concerned."

When talking about cases regarding the leakage of consumer personal data, of course, there will be no agreement from the person concerned, that other parties can access their personal data, or it can be said that the use of personal data is carried out without the knowledge of the person concerned. For example, in the case of Tokopedia in early May 2020, Tokopedia experienced a data leak of 15 million consumer accounts. The account that leaked also said it owned and would sell 91 million consumer data for Tokopedia users. The data, which was previously traded for USD 5,000 or around Rp. 70 million, can now be downloaded freely (JawaPos, 2020).The leak of consumer data is due to the fact that Tokopedia was hacked by an international hacker with the nickname "*Why So Dank*". According to @underthebreach, the hacked data contained emails, passwords, and usernames from Tokopedia consumer accounts. The Tokopedia case is an example of a violation of Article 26 paragraph (1) of the ITE Law which explains that consumer personal data should be protected and cannot be accessed or used by other parties without the consent of the person concerned, in fact in the Tokopedia case consumer data can be accessed freely and can be traded.

However, in fact, when there is a leak of consumer data, there has been no settlement or civil liability carried out by parties proven to have violated these rules, either through the provision of compensation or other sanctions to the injured party. And the ITE Law does not explain further regarding sanctions for these violations.

Other regulations that regulate further related to the provisions of Article 26 Paragraph (1) are contained in Article 26 of the Minister of Communication and Informatics No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems. The article also explains the rights of the owner of personal data. Article 26 letter (a) which states that the owner of personal data has the right to the confidentiality of his personal data, in the case of leakage of personal data that violates the rights of consumers as owners of personal data, the rights of consumers who are violated are the rights regulated in Article 26 letter (a) which states the owner of the data. Personals have the right to the confidentiality of their personal data, this right is violated because the confidentiality of consumer personal data is lost due to leakage of personal data to third parties. However, Permenkominfo No. 20 of 2016 also does not explain the sanctions/punishments or forms of responsibility related to the violation of Article 26 letter (a).

The existence of sanctions or penalties for actions that violate the provisions of Article 26 Paragraph (1) of the ITE Law or can be called a violation of the leakage of consumer personal data is one form of responsibility that should be carried out by the violating party. When a consumer's personal data leaks, it will cause some material losses to the data owner including:

1. If personal data is leaked, it can be used to break into financial accounts
2. Leaking personal data allows the creation of accounts whose owners don't feel like creating
3. Can be used to apply for an online loan
4. Profiling for political targets or social media advertising
5. Personal numbers traded for telemarketing

With a loss to someone in this case the data owner, due to the fault of the party who violates the provisions of the legislation, the party must be civilly responsible to the injured party. However, in this case, there is no further regulation regarding the civil responsibility.

Regarding the leakage of consumer data, it can be seen from the perspective of Islamic Economic Law. The study of Islamic economics in Indonesia is increasingly finding its relevance to practical needs after the birth of various supporting regulations, including Law no. 3 of 2006 concerning the Religious Courts (which gives absolute authority to the Religious Courts to resolve sharia economic disputes) Law no. 21 of 2008 concerning Islamic Banking and Perma No. 2 of 2008 concerning the Compilation of Sharia Economic Law and so on. Seeing from the perspective of other laws that both have rules related to an act that gives rise to accountability will enrich the view in interpreting and solving a problem. In addition, in its development, *fintech* is not only in conventional form but also in sharia.

The problems raised in this study, found several related journals that have the same theme, namely:Rati sanjaya and Irwansyah, "Ethics and Privacy of Financial Technology Services (*Fintech*) Phenomenological Studies on Victims of *Fintech* Privacy Violations" Journal Communication Spectrum: Capturing New Perspective in Communication, Vol. 9 No. 1 February-July 2019, University of Indonesia. The focus of the discussion in this journal is on ethics and privacy values that must be considered in the implementation of *fintech* and the impact that arises when the implementation of *fintech* is not in accordance with ethics and privacy values (Rati Sanjaya, 2019).The difference is that previous research focuses on ethics and privacy in the implementation of *fintech*, with research conducted empirically. While this research focuses on the form of responsibility from *fintech* companies to service users when data leaks occur, and this research was conducted using a library study.

Ana Sofa Yuking, "The Urgency of Personal Data Protection Regulations in the *Fintech* Business Era" Journal of Law & Capital Markets. Vol. VIII. Ed. 16/2018. The focus of this journal is related to the urgency of personal data protection in the *fintech* business through the PDP Bill (Ana Sofa, 2018).The difference with previous research is in the focus of the research, which focuses more on the urgency of the existence of personal data protection in the *fintech* business through the PDP Bill. Meanwhile, this research focuses on the form of accountability from *fintech* companies to service users when data leaks occur.

Ni KadekPuspaPranita and I Wayan Suardana, "Legal Protection for Customers Using *Fintech* Services (Financial Technology) KerthaSemaya: Journal of Legal Studies, v. 7, n. 2, p. 1-16, july 2019. The discussion in this journal focuses on forms of legal protection for customers using *fintech* services and the role of OJK in the implementation and development of *fintech* businesses (Ni Kadek, 2019).The difference with previous research is in the focus of previous research on forms of legal protection and the role of OJK in the implementation and development of the *fintech* business. While this research focuses on the form of accountability from *fintech* companies to service users when data leaks occur

Regarding the form of civil responsibility that must be carried out in the event of a consumer data leak in the business *fintech*never been discussed before.

II. DISCUSSION

In general, the parties in financial technology consist of operators in the *fintech* business, every party participating in the implementation of *fintech* and users of *fintech* services. The agreement on *fintech* should be the same as the agreement in general, where the agreement entered into must meet the legal requirements of the agreement, one of which is the agreement of the parties (Ariyani, 2013).

Terms and Conditions (*Terms & Conditions*) are rules set by several *fintech* companies, one of which is the case, namely Tokopedia as a service provider. The stipulated terms and conditions govern the use of services related to the use of the www.tokopedia.com site. Consumers who register and/or use the www.tokopedia.com site are deemed to have understood and agreed to the contents of the terms and conditions. These terms and conditions basically act as an electronic agreement (e-contract) for the parties. This form of electronic agreement is known as a click-wrap agreement (DekyPariadi, 2018).In e-contracts, generally an agreement is reached when the consumer clicks on the agreement section (LathifahHanim, 2018).A click-wrap agreement is a contract for the purchase of goods or the use of goods or services offered by an online merchant. In general, online buyers must agree to the terms stated in the standard contract that has been prepared by clicking the icon, (which usually contains the words I agree, I Accept, OK, Agree) before completing the transaction.

It can be seen that in general a contract will be born when there is acceptance of an offer. This is not much different from an electronic contract, the birth of an electronic contract in principle has similarities with a conventional contract. Electronic agreements in *fintech*, born through their website which has provided financial service forms or financial products that can be filled directly by prospective debtors as needed or prospective debtors open an account then register to become a member before getting the form and verifying data via e-mail (Edy Santoso, 2019).

The legal relationship between the operator and *fintech* users in this case occurs because of the approval of an electronic agreement. Where the electronic agreement in *fintech* contains the rights and obligations of the parties. The obligations of *fintech* operators here are based on Article 30 of the 2018 POJK, namely the Operators are required to maintain the confidentiality, integrity, and availability of personal data, transaction data, and financial data that they manage from the time the data is obtained until the data is destroyed. For the use of user data and information obtained by the operator, the operator must obtain approval from the user, convey the limits on the use of data and information to the user, convey if there is a change in the purpose of using data and media information and the method used to obtain data and information, guaranteed all confidentiality, security,Meanwhile, the obligation of *fintech* service users is to provide correct personal data or information to *fintech* business operators (Mansyur, 2009). The rights of *fintech* users are to obtain financial services offered by *fintech* providers and to get guaranteed legal protection for the security of their personal data that has been submitted (Yudha, 2020).

If it is related to the obligations of the *fintech* business operator against the leakage of consumer personal data, the provider (*fintech* business operator) has an obligation to store personal data to prevent leakage or prevent any processing activity or use of personal data that is against the law and is responsible for unexpected losses or damages. what happened to the personal data, this has been stated in Article 59 Paragraph (2) letter (g) of PP No. 80 of 2019. Thus, based on the factors, impacts, and provisions above, *fintech* business

operators as mandated bearers of their users' personal data have an obligation to maintain the security and confidentiality of user data (Muhammad Hasab, 2020).

Due to the leakage of consumer personal data that occurred in Indonesia, *fintech* business operators who act as mandates for the use of consumer personal data should be held accountable for the leakage of personal data experienced by users. In this case, it can be categorized as an act that violates the law and is held accountable if it has fulfilled the elements of a violation of the law that have been regulated in the legislation.

When described, the elements of the leakage of personal data of *fintech* users are as follows: 1) There is an act, in this case the act that occurs is the occurrence of a leak of personal data of consumers of *fintech* business users; 2) The act violates the law, it is clear that in this case the act that occurs is an unlawful act, because there are norms that are violated by *fintech* business operators, Article 59 PP 80 of 2019 concerning Trading Through Electronic Systems has stated that business actors are required to store personal data in accordance with personal data protection standards or common business practices, the party storing personal data must have a proper security system in place to prevent leakage or prevent any unlawful processing or use of personal data and be responsible for any unexpected loss or damage that occurs to the personal data; 3) There is an error from the perpetrator, the fault of the *fintech* business operator is the lack of the principle of prudence in the process of storing consumer personal data, causing the leakage of personal data. Article 3 of Law Number 11 of 2008 concerning Information and Electronic Transactions has emphasized the principle of prudence and also gives responsibility to every Electronic System Operator, both corporate and government, to implement electronic system accountability, which must be reliable, safe and responsible; 4) There is a loss to the victim, the loss to the victim can be seen with the naked eye, where his personal data is owned by people not with his consent, for example there is interference from telemarketers and criminal attempts such as fraud or Sim Swap or other crime modes; 5) There is a causal relationship between actions and losses, when viewed from the background of the leakage of personal data of *fintech* user consumers, this is caused by the actions of *fintech* business operators who do not fulfill their obligations according to the applicable norms, resulting in losses to consumers who use them.

Based on the fulfillment of the elements of unlawful acts as mentioned above, a responsibility for *fintech* business operators is born. In the provisions of Article 59 of PP 80 of 2019 it has been stated that business actors are required to store personal data according to personal data protection standards or the prevalence of developing business practices. From the provisions of this article, it can be seen that there are norms that require *fintech* business operators to always guarantee the security of consumer personal data that has been given to them (AA Ngurah, 2021).

Thus, the occurrence of the leakage of consumer personal data becomes his responsibility even though the incident was not against his will, but due to errors and lack of caution in the application of a personal data security system that resulted in the leakage of personal data of his consumers. Article 3 of Law Number 11 of 2008 concerning Information and Electronic Transactions has emphasized the precautionary principle and also gives responsibility to every Electronic System Operator, both corporate and government, to implement electronic system accountability, which must be reliable, safe and responsible.

Based on Article 26 of the Minister of Communication and Informatics No. 20 of 2016 explains the rights of the owner of personal data or in the case of leakage of personal data, the owner of personal data is the consumer. Leakage of consumer personal data violates the rights of consumers as owners of personal data, the rights of consumers that are violated are the rights regulated in Article 26 letter a which states that the owner of personal data has the right to the confidentiality of his personal data, this right is violated because the confidentiality of consumer personal data is lost due to leakage of personal data to third parties. Permenkominfo No. 20 of 2019 does not explain sanctions or penalties related to violations of Article 26 letter a, but Article 26 letter b explains that consumers as owners of personal data can file complaints for the failure to protect the confidentiality of personal data carried out by PSE (Electronic System Operator) to the Minister of Communications and Informatics Republic of Indonesia (Siti Yuniarti, 2019).

Based on the provisions of Article 26 Paragraph (2) of Law Number 16 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, it has provided

an explanation that any victim whose rights are violated can file a civil lawsuit based on this law. The right type of liability applied to *fintech* business operators is fault liability. Responsibility with elements of error (intentional and negligence) as stated in Article 1365 of the Civil Code. Accountability contained in Article 1365 of the Civil Code and Article 1366 of the Civil Code requires an element of error, meaning that a person must be guilty (*liability based on fault*), (Velliana, 2019). The principle of accountability in error is based on the principle that there is no accountability if there is no element of error in the science of law called *Tortious Liability* or *Liability Based on Fault*. Furthermore, the party who is obliged to prove the element of error is the party who demands compensation in other words the burden of proof is on the plaintiff as determined by Article 1865 of the Civil Code "everyone who argues that he has a right, or, in order to confirm his own right or refute a rights of others, referring to an event, are required to prove the existence of such rights or events."

Furthermore, regarding accountability in an organ (company), Hoge Raad adheres to the organ theory which explains that a legal entity can be held civilly responsible under Article 1365 of the Civil Code if the organ commits an unlawful act. If an organ acts to fulfill the task assigned to it and subsequently the action turns out to be against the law, then the organ's actions are considered as an act of a legal entity and the legal entity must be held responsible. So that the civil liability of legal entities can be directly based on Article 1365 of the Civil Code and indirectly (if carried out by organs/subordinates) based on Article 1367 of the Civil Code.

The problem in the previous discussion is that it is known that data leakage that occurs to consumers using *fintech* services is a mistake made by the *fintech* company as the party responsible for implementing the implementation of the electronic system. As explained at the beginning that related to data leakage, it is regulated in the ITE Law Article 26 paragraph (1) which relates to consumer rights that must be fulfilled by the electronic system operator, of course if it is a right that must be fulfilled by the party who is obliged to carry out this but cannot be implemented, there will be other responsibilities that must be fulfilled. Legally, this responsibility has been explained in the previous discussion.

The previous discussion explained that consumer data leakage is a loss for consumers who use *fintech*. In the perspective of Islamic Economic Law, all actions that cause harm to others are included in acts against the law in Islam, this act is called *Al-fi'lu Al-dharar* (harmful actions), (Imron, 2019).Another term used to refer to the term unlawful act other than *al-fi'lu al-dharar* is *al-'udwân* which gave birth to *dhamân al-'udwan* (satisfacion guarantee of trespass) or also *al-taqshîr* (reckless act) which gave birth to *mas'ûliyyah al-taqshîriyyah* and also *amalghar al-masyrû*. Thus, an unlawful act can be defined as an act that is not in accordance with the provisions of the law that harms other parties and creates responsibility (*dhamân*) for the perpetrator.

*Al-fi'lu Al-dharar*can occur if the elements of *Al-fi'lu Al-dharar*are met, namely: 1) the element of action; 2) elements against the law; 3) the element of error; 4) the element of loss; 5) the element of a causal relationship between errors and losses.

In the first element, namely the element of action, what is meant in this element is *Al-fi'luNafi'*, namely actions that are useful according to propriety. A person who sees a situation in which according to propriety he should do (must do) something for good, and if it is not done it will cause harm to the other party (which is the right of the other party) then the law attaches an obligation to him to do the act as appropriate. To determine the measure of propriety, the theory of Islamic law uses the *'urf* (customary) approach. If custom requires someone to do or not do something, then it has the power of law. The concept of *'urf* in Islamic law is recognized for its existence and can even be taken into consideration in determining the law.

In the second element, related to the element of violating the law, actions that are contrary to prudence or necessity in good social relations are also considered as acts against the law. If a person commits an action that harms another person, does not violate the articles of written law, he can sue him with an unlawful act because his action is contrary to the precautionary principle or necessity in social interaction. Acts that are contrary to prudence or necessity in good social relations are also considered as acts against the law. If a person commits an action that harms another person, does not violate the articles of written law, he can sue him with an unlawful act because his action is contrary to the precautionary principle or necessity in social interaction. This obligation in the community is certainly not written, but is recognized by the community concerned. Morality

means decency related to manners and manners. Susila means good manners, civilized, polite, orderly, good customs, manners. Good decency is what can be stated as a moral norm or which can be socially accepted as a legal norm.

The third element is due to an error, in the context of an unlawful act, the error referred to here includes the context of doing something such as intentionally burning, drowning, or destroying, and also not doing something, such as being silent when the item entrusted is taken by someone else. Other types of errors are direct errors such as cutting someone else's tree without rights, or indirect errors such as making a well on a public road without a permit which then causes the vehicle to fall in it. An act that can be categorized as an unlawful act in the perspective of Islamic Economic Law is if the act violates the habits of people in general, not the habits of people who are too stupid or too smart. It's the same with mistakes made when a data leak occurs, where personal data that should be guarded and may only be accessed with the permission of the owner can in fact be freely accessed by other parties without permission and without the knowledge of the owner. In the study of Islamic law, mistakes in unlawful acts do not look at whether intentional or not, even when the error is committed by those who are old enough or not old enough, then the person concerned must still be responsible for compensation, except for the Malikiyyah school which states that the child minors who are not yet *mumayyiz* are not obliged to provide compensation when damaging/losing other people's goods.

In determining the degree of guilt for one's actions, Islamic law uses the theory of motivation (intentions). An act that has been done has different legal consequences, when the underlying motivation is different. Ibn Qayyim al-Jauziyyah said that an action may or may not be permissible depending on the underlying motivation. Motivation as the basis for determining the severity of an error is based on the generality of the hadith which states that in fact every action is measured in its motivation (*innamâ al-'amâl bi al-niyât*). Based on this hadith, fiqh rules were developed which state that everything is based on motivation (*al-umûrbimaqâshidiha*).

In the fourth element, there is a loss. The existence of a loss is basically the core of the discussion of the responsibility for compensation. Because even if there is an error, if there is no loss, then there is nothing to replace. Amran Sadi provides information regarding 4 (four) conditions that must be met so that the loss can be used as a reason to ask for compensation, namely:1) The loss according to custom and sharia can be assessed as property. Thus, non-wealth such as a handful of land is not included in this category; 2) Has a value/price in the Shari'a scales, so in this case goods such as alcohol (alcohol) which basically have no price in Islamic law cannot be used as the basis for a loss; 3) Owned, then there is no loss in things that no one owns, for example water from a spring; 4) *Muhtaram* (protected), then there is no loss in the goods owned by the enemy during the war (H. Firmanda, 2018).

The last is the element of a causal relationship between errors and losses. In Islamic Economic Law, causality here is divided into 2 (two) types, namely direct (*mubâsyarah*) and indirect (*tasabbub*). Direct causality is when one person's actions towards another are directly related to the harm that occurs. As for indirect causality, there is an association between the results/forms of one's actions and the losses suffered by others. It is important to distinguish between the two because this relates to the compensation that will be given.

Islamic jurists divide the causes into 3 (three) parts. First, sensory causes, that is, causes that clearly and unquestionably give rise to effects, either directly or by other causes arising from the first cause. For example, someone who intentionally parks a car near a fire that is spreading, even though his actions do not immediately burn the car, but by placing the car near the fire causes the car to catch fire. Second, *syar'iy* causes, namely causes that cause consequences for which the perpetrator must be held responsible based on the provisions of *syara'*. For example, false testimony before a judge that results in a person being sentenced to a criminal sentence or defeated in a civil dispute. In this case, the perpetrator must be held accountable based on the provisions of *syara'* even though the consequences of his actions have passed. Third, *urfi* causes, namely causes that have no effect other than these two things. In other words, the cause of *urfi* is a cause whose causality is based on the habits of people's minds. Based on the theory of *urfi* causes, the perpetrator must be responsible for the consequences of his actions, even though the causes are sequential, if habit requires such accountability. For example, in a ship there is someone who deliberately makes a hole in the wall of the ship.

When the ship started to tilt, some of the passengers jumped out and were eaten by the sharks. Even though the act was not the direct cause of the victim's death, the act of perforating the ship can be held accountable for the victim's death.

The application of cause based on this *urfi* theory helps to find the causality between cause and effect to be elastic. Based on Article 451 paragraph (2) of the Compilation of Sharia Economic Law (KHES). In the event that there are two indirect causes, the judge decides which cause caused the damage or depreciation.

If viewed from the explanation of these elements, from the perspective of Islamic Economic Law, leakage of consumer personal data can be categorized as Al-fi'lu Al-dharar (harmful actions) or unlawful acts. Because of the five elements that must be met in order to be said to have violated the law in this matter, it is fulfilled. If it is described as follows: First, the obligation of propriety as an electronic system operator has been attached to maintain the confidentiality of consumer's personal data; secondly, data leakage is an act that is contrary to prudence or necessity in good social relations; third, the occurrence of data leakage is an error made intentionally or not by the electronic system operator, either directly or indirectly; Fourth, from the data leak, the data owner suffered losses, for example, it was used to break into financial accounts, besides that victims of personal data theft for borrowing (a type of *fintech*) not only experienced financial losses, but also psychological fear and wasted energy because they had to deal with legal services. to get help; fifth, because the data leak has causality with the losses received by the data owner as mentioned in the previous point.

Therefore, in the perspective of Islamic Economic Law it is included in the category against the law. In Islamic Economic Law, an act against the law has an accountability called *dhamân* (accountability) or *ta'widh* (compensation). The concept of *dhamân* in Islamic Economic Law has the purpose of eliminating harm, that is, eliminating the losses suffered by the aggrieved party due to default or acts against the law. There is a value of balance in the concept of *dhamân* in Islam, which is the balance of worldly matters and the hereafter. The things of the world, the concept of *dhamân*are related to the psyche, honor as well as possessions. As for the matter of *ukhrawi*, the concept of *dhamân* is a *dain* (debt) that must be paid so as not to be implied as a demand in the hereafter.

In the study of Islamic Economic Law, legal responsibilities are divided into 2 (two), namely (1) *dhamân al-'udwan*, namely responsibility for actions that harm others (legal acts); and (2) *dhamân al-'aqd*, namely civil responsibility to provide compensation that stems from acts of default or acts against the law. Islamic Economic Law experts formulate the types of compensation are divided into 2 (two) types, namely: first, *al-dharar al-mâddi* (material loss), namely the loss that befell a person's property; and second, *al-dharar al-ma'nawi* (immaterial loss).

Based on the element of harm to others, it will arise as a result of the law in the form of compensation, which in Islamic Economic Law is called the term *ta'wîdh*. Wahbah al-Zuhaili in the book Nadzariyyat al-Dhâman explains that what is meant by *ta'wîdh* is as follows: "Covering the losses that occur caused by acts of ta'adî (extreme acts) and khatâ (mistakes)".The focus of the discussion on *ta'wîdh* is how to eliminate material losses due to unlawful acts, so that the party who suffers the loss can be returned to its original condition. The form of return can be in the form of returning damaged goods to their original state and if this is difficult or even impossible to do, then it is done in the form of compensation payments (F. Wahyudi, 2017).

Compensation or *ta'wîdh* has the meaning of real compensation for errors that occur. In the Compilation of Sharia Economic Law (KHES) Article 20 paragraph 37 it is stated that compensation (*ta'wîdh*) is compensation for real losses paid by parties who have defaulted or violated the law. The Indonesian Ulema Council (MUI) through the National Sharia Council (DSN) has issued fatwa No. 43/DSN-MUI/VIII/2004 concerning Compensation (*ta'widh*). The fatwa is not only shown to parties who default in sharia contracts, but can also be used as a legal basis for unlawful acts. A loss can be caused by an unlawful act (*al-fi'l al-dharar*), so that it implies a loss to others and can also be caused by a default. Losses caused by unlawful acts, the perpetrator is obliged to provide compensation for the actions he has committed (Hasanuddin, 2020)

In determining compensation, must consider various things. There are 4 (four) principles that must be considered in relation to claims for compensation in the perspective of Islamic economic law. First, the principle of *al-yusr* (make it easy) in calculating and measuring compensation to avoid lengthy processes and procedures

in court so that justice seekers do not wait too long for their rights; second, consistent, namely that there is uniformity in the quality and quantity of compensation in the same case; third, equating (*al-musâwah*) between all occupations in receiving compensation. The principle of equality before the law is part of what gives birth to justice; and fourth, must first identify and determine the level of involvement of the actors.

In essence, what must be done by each individual in *muamalah* according to the basic principles of Islamic Economic Law is *lâdhararwalâdhirâr*, meaning that Islamic law prohibits dangerous and harmful acts. Therefore, every action that harms others, whether intentionally or not, the perpetrator must be responsible for all damage and losses that arise. If the perpetrator is unable to provide compensation or damage caused by his actions, such as crazy people and children who are still not yet mature, the responsibility must be borne by the guardian. The obligation to provide compensation in Islamic Economic Law aims to protect and preserve property from all destruction and destruction and to provide a sense of security to the owner from things that are harmful.

Even in the Qur'an there is more than one verse that instructs that every action that can harm another person should be compensated accordingly. This is explained, among others, in the Qur'an surah al-Baqarah (2): 194 which means "Whoever attacks you, then attack him, equal to the attack on you".

III. CONCLUSION

Based on the provisions of Article 59 of PP 80 of 2019 which states that business actors are required to store personal data according to personal data protection standards or the prevalence of developing business practices, then from the provisions of this article there is a norm that obliges *fintech* business operators to always ensure the security of consumer personal data. has been given to him. So that when a consumer's personal data leak occurs, it becomes his responsibility even though the incident was not against his will, but due to errors and lack of caution in terms of implementing a personal data security system which resulted in the leakage of the consumer's personal data. Article 3 of the ITE Law has emphasized the precautionary principle and also gives responsibility to every Electronic System Operator, both corporate and government, to implement electronic system accountability, which must be reliable, safe and responsible. Based on the provisions of Article 26 Paragraph (2) of Law Number 16 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, it has provided an explanation that any victim whose rights are violated can file a civil lawsuit based on this law. The right type of liability applied to *fintech* business operators is fault liability. Accountability for errors is contained in Article 1365 of the Civil Code and Article 1366 of the Civil Code with the principle of faulty responsibility based on the principle that there is no liability if there is no element of error.

Leakage of consumer data is a loss experienced by consumers who use *fintech*. All actions that cause harm to others are included in unlawful acts in Islamic Economic Law, this act is called *Al-fi'lu Al-dharar* (harmful actions). In Islamic Economic Law, an act against the law has an accountability called *dhamân* (responsibility) or *ta'widh* (compensation). The concept of *dhamân* in Islamic Economic Law has the aim of eliminating harm, namely eliminating the losses suffered by the injured party due to default or unlawful acts. Legal responsibilities are divided into 2 (two), namely (1) *dhamân al-'udwan*, namely responsibility for actions that harm others (lawful acts); and (2) *dhamân al-'aqd*, namely civil liability to provide compensation that stems from acts of default or acts against the law.

REFERENCES

[1] Rian Alfianto, (2020). "91 Million Tokopedia Account Data Leaked and Distributed in Internet Forums," Jawa Pos, https://www.jawapos.com/oto-dan-tekno/technology/05/07/2020/91-juta-data-akun-tokopedia-bocor-dan-disebar-di-forum-internet/

[2] Rati sanjaya and Irwansyah, (2019). Ethics and Privacy of Financial Technology Services (*Fintech*) Phenomenological Studies on Victims of *Fintech* Privacy Violations, *Journal of Communication Spectrum: Capturing New Perspective in Communcation*, 9, 34-42.

[3] Ana Sofa Yuking, (2018). The Urgency of Personal Data Protection Regulations in the *Fintech* Business Era, *Journal of Law & Capital Markets*, 8*(16)*, 76-84.

[4] Ni KadekPuspaPranita and I Wayan Suardana, (2019). Legal Protection for Customers Using *Fintech* Services (Financial Technology), *KerthaSemaya: Journal of Legal Studies, 7(2)*, 1-16.

[5] Ariyani E, (2013). *Covenant Law*. Yogyakarta: Ombak Publishers.

[6] DekyPariadi, (2018). Supervision of E-Commerce in the Trade Law and Consumer Protection Act, *Journal of Law and Development*,48*(3)*, 76-84.

[7] LathifahHanim, (2018). Legal Protection for Parties in E-Commerce As a Result of Economic Globalization, *Journal of Legal Reform*, 1*(2)*, 90-111.

[8] Edy Santoso, (2019). Legal Review of Click Wrap Agreements on Electronic Standard Contracts Related to Electronic Transactions, *Scientific Journal of Living Law*, 7*(1)*, 76-80.

[9] Mansur, DMA, and Gultom, E, (2009). *Cyber Law Legal Aspects of Information Technology*. Jakarta: PT. RefikaAditama.

[10] Yudha, ATRT et al, (2020). Fintceh Syariah: Theory and Application. Surabaya: Scopindo Media Pustaka.

[11] Muhamad HasabRumlus, (2020). Policy on Combating Personal Data Theft in Electronic Media, *Journal of HAM*, 11*(2)*, 102-119.

[12] AA NgurahDeddy Hendra Kesuma, I Nyoman Putu Budiartha& Putu Ayu SriasihWesna, (2021), Legal Protection Against Personal Data Security of Financial Technology Consumers in Electronic Transactions, *Journal of Legal Preferences*, 2*(2)*, 98-117.

[13] Siti Yuniarti, (2019), Legal Protection of Personal Data in Indonesia, *Becoss Journal (Business Economic, Communication, and Social Sciences)*,1*(1)*, 56-69.

[14] VellianaTanaya, (2019), Reconstruction of the Principles of Unlawful Acts in Consumer Disputes, *Journal of Sharia and Asy-Syir'ah Law*, 47*(1)*, 125-132.

[15] ImronRosyadi, (2019). *Sharia Nominated Contracts: Implementation and Dispute Resolution*. Jakarta: KencanaPrenada Media Group.

[16] H. Firmanda, (2018), The Nature of Compensation in the Perspective of Sharia Economic Law and Indonesian Civil Law,*Journal of Law Respublica*, 17(4), 77-90.

[17] F. Wahyudi, (2017), Controlling Customer Moral HazardThrough Ta'Zir and Ta'Widh Instruments,*Al-Banjari: Scientific Journal of Islamic Sciences*.

[18] Hasanuddin, Fakhruddin Mansyur, (2020). M. M. MUI DSN Fatwa Clause of Fines and Compensation on the Sharia Mortgage Scheme (DSN MUI Fatwa on the Clause of Fines and Compensation on the Sharia Mortgage Scheme, 7(2).