UNTAG Law Review (ULREV)
Volume 8, Issue 2, Oktober 2024, PP 119-130
ISSN 2549-4910 (online) & ISSN 2579-5279 (print)
http://jurnal.untagsmg.ac.id/indeks.php/ulrev/indeks
www.fakhukum.untagsmg.ac.id

LAW ENFORCEMENT AGAINST CRIMINAL ACTS OF FRAUD USING THE ONLINE INVITATION MODE

Ismiyanto[1]
[1]Department of International Law, University 17 August 1945 Semarang, Indonesia
[1]ismiyanto.ca@gmail.com

ABSTRACT; The most popular case of online fraud is fraud using online invitation mode on social media. Law enforcement against criminal acts of fraud using online invitation mode is very important. Lack of strict and clear law enforcement is the trigger for this criminal act of fraud to continue to occur. This research aims to describe the regulation of criminal acts of fraud in Indonesian law and analyze law enforcement against criminal acts of fraud using the online invitation mode. This type of research is normative legal research. This research uses a statutory approach. The data source for this research uses secondary data. The data analysis technique used is qualitative data analysis technique. The research results show that criminal acts of fraud in Indonesian law are regulated in the Criminal Code and the Information and Electronic Transactions Law. In the Criminal Code, fraud is regulated in Chapter XXV Book II of the Criminal Code Articles 378-395 and specifically regulated in Article 378 of the Criminal Code, online fraud is regulated in Article 28 Paragraph (1) of the Information and Electronic Transactions Law. The online invitation mode for criminal fraud is relatively new. Law enforcement is carried out by the Police against perpetrators of fraud using the online invitation mode, namely arresting perpetrators who create online invitation applications. Law enforcers usually impose multiple articles as regulated in Article 378 of the Criminal Code and Article 28 Paragraph (1) of the Information and Electronic Transactions Law with the threat of imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of IDR. 1,000,000. 000, to prove error, Article 5 and Article 6 of the Information and Electronic Transactions Law are used as recognition of information, documents and electronic signatures as valid evidence in court.

Keywords: *Keywords: Mode, Fraud, Online Invitation*

INTRODUCTION

Current technological developments are not just for the sake of communicating and socializing, but also lead to a world network without borders.(Dendi Pajriansyah, 2023) Advances in information technology, including telecommunications, are not only occurring in developed countries, but also in developing countries. Indonesia is one of the countries whose technology is currently developing rapidly, including in the fields of science, social, economic and cultural fields.(Darmayanti, n.d.) One of the results of technological advances is the use of the internet.

The application of internet technology has touched all aspects of people's lives. This advanced technological progress has had a positive impact on various lives, as it is e-mail, e-commerce, e-learning, EFTS (Electronic Funds Transfer System atau sistem transfer dana elektronik), internet banking, cyber bank, on-line business etc.(Mus Muliadin, n.d.) The development of internet technology can also have negative impacts. One of the negative impacts caused by technological developments is the emergence of the threat of modern crimes.(Sakti, n.d.) Crime continues to grow along with the development of human civilization, with complex quality and quantity and variations in modus operandi.(Wahyuni, 2017) Through the internet, several types of criminal acts are becoming easier to commit, such as criminal acts of defamation, pornography, gambling, account burglary, cyber network destruction (hacking), attacks via viruses (virus at-tack) and so on.(Maskun, 2013)

Crimes caused by the development and progress of information and telecommunications technology are crimes related to internet applications or in foreign terms called cyber crime. The definition of cyber crime is more general crime which has the characteristics of being carried out by parties who control the use of information technology such as the internet and mobile phones.

The level of cyber crime in Indonesia is ranked second in the world. In Indonesia, 6,388 cases of cyber crime have been reported from 2019 to May 22 2020. Most of these crimes took the form of spreading provocative content, namely 2,584 reports. Meanwhile, the second most common crime received by cyber patrols was online fraud with 2,147 cases.

Cybercrime increased significantly in 2022 when compared to the same period in 2021, in fact the number of cybercrimes increased by 14 (fourteen) times. Data on the e-MP Robinopsnal Bareskrim Polri shows that the police took action against 8,831 cybercrime cases from January 1 to December 22 2022. All work units at Bareskrim Polri and Polda in Indonesia took action against these cases. Polda Metro Jaya is the work unit with the highest number of prosecutions for cybercrime cases, namely 3,709 cases. Meanwhile, in the same period in 2021, the number of prosecutions was 612 throughout Indonesia. Only 26 work units took action.

One of the crimes using online media is fraud. Not much different from in cyberspace, online fraud is rampant in society. Online fraud is a form of crime that uses technological facilities in every action. The principle of online fraud is the same as ordinary or conventional fraud, where in every case of fraud there is a victim who is harmed and another party benefits illegally. The difference between online and conventional fraud is the use of electronic systems (telecommunications devices, internet and computers).(Rahmad, n.d.)

Indonesia is one of the countries with the largest number of victims of online fraud in the world. It is recorded that as many as 26 percent of consumers in Indonesia have been victims of online fraud. Data available from 2016 to 2020 records a total of 7,047 cases of online fraud reported and online fraud has a percentage of 28.7% of total cyber crimes. (Zabindin, 2021) This condition makes Indonesia one of the countries with the largest number of victims of online fraud in the world.

The case of online fraud that is currently popular is fraud using online invitation mode on social media. The mode of fraud in electronic wedding invitations that is distributed via messages is becoming increasingly common, which is quite disturbing to the public. The perpetrator of this fraud committed fraud by embedding an APK application document in the application file format for Android phones with the name of a digital wedding invitation letter. If you are not careful, the recipient will not know that the document being shared is a fake invitation used to break into the victim's personal data and access banking data. Electronic wedding invitation fraud can also occur via text messages (SMS) or direct messages on social media platforms. These scammers often use very persuasive techniques, such as claiming that the invitation is limited or that there is a special offer that is only valid for a certain time. This can trick unsuspecting potential guests and get them caught in a scam trap.

Law enforcement against criminal acts of fraud using online invitation mode is becoming increasingly important considering the social and economic impact caused by this criminal act. Victims often experience financial losses, as well as psychological losses due to privacy violations and loss of trust in cyberspace. Lack of strict and clear law enforcement against perpetrators of criminal acts of fraud using the online invitation mode is often the trigger for these criminal acts of fraud to continue to occur.

The issues that will be discussed are how to regulate criminal acts of fraud in Indonesian law and how to enforce the law against criminal acts of fraud using the online invitation mode. Theoretically, this research is expected to be useful for the development of legal science, especially criminal law, in order to expand knowledge and add references regarding matters relating to law enforcement against criminal acts of fraud using the online invitation mode and practically, the results of this research are expected to be useful for all both academics and legal practitioners, law enforcement officials, the general public, and other parties related to law enforcement against criminal acts of fraud using the online invitation mode.

PROBLEM

1. The problem that will be discussed is how is the criminal act of fraud regulated in Indonesian law?
2. How is law enforcement against criminal acts of fraud using online invitation mode?

RESEARCH METHODS

This type of research is normative legal research, namely a legal research method carried out by examining library materials or secondary materials,(Muchtar, 2015) also called doctrinal research. This legal research is prescriptive in nature, the legal process which includes inquiry, inquiry, prosecution and court decision (condemn or

acquit), is a form of prescriptive research.(Irwansyah, 2022). This research uses a statutory approach. The legislative approach is an approach by analyzing or reviewing legal rules such as laws based on positive law in Indonesia or those currently in force.(Marzuki, 2014) A legislative approach is carried out by reviewing all laws and regulations that relate to the legal issue being raised.(Efendi, 2018) The data source for this research uses secondary data. Secondary data is data obtained from official documents, books related to research objects, research results in the form of reports, theses, theses, dissertations, and statutory regulations.(Rokilah, 2020) Secondary data in the legal field is further divided into 3 (three) types based on their binding strength, namely primary material, secondary legal material and tertiary legal material.(Azhar, n.d.) The data analysis technique used in this research uses qualitative data analysis techniques. Analysis was carried out to develop a theory based on the data obtained,(Abdussamad, 2021) which ends with a conclusion.(Saleh, 2017)

DISCUSSION

Regulation of criminal acts of fraud in Indonesian law

Fraud is a crime that can be committed by everyone, both poor and rich, and all ages and all genders can commit this crime. This is because the motives of each perpetrator are also different. The victims also vary, but tend to be people who own property as the targets of this crime. It is also possible that something else could be a target for fraud, including personal data, actions of the victim that could be profitable, the victim's intellectual property and so on.

Fraud as a complaint offense, the victim must report that he or she has been a victim of fraud. The victim is usually one person or even many people depending on the method and how massive the fraud is in society. It is also possible that the perpetrator is more than one person who is usually organized because the method used requires involving many people so that the criminal act is disguised.

Fraud as a financial crime has developed in various modes, ranging from simple to complex scales and even involving organized or corporate actors. Fraud is very widespread as time goes by. This happens because fraud is easy to commit. The fraudster only needs to convince the victim with lying words so that the victim will do or follow what the fraudster wants.

Actions in the context of criminal law can be said to be fraud if they fulfill the formulation of Article 378 of the Criminal Code. In Article 378 of the Criminal Code, the crime of fraud (oplichthing) is stipulated in a general form, while what is stated in Chapter XXV Book II of the Criminal Code contains various forms of fraud against property which are formulated in several articles, each of which has specific names (fraud in special form). The entire article in Chapter XXV is known as bedrog or fraudulent acts. The criminal act of fraud or bedrog contained in Articles 378-395 of the Criminal Code Chapter XXV is fraud in the broad sense, whereas in Article 378 of the Criminal Code states the term oplichting which has the meaning of fraud in the narrow sense.

The elements of a criminal act of fraud are as follows:(Manalu, n.d.)

1. The element of moving other people is actions, whether in the form of actions or words that are deceptive.
2. The element of handing over an object. Handing over an object does not have to be done directly by the person who is being deceived to the person who is deceiving him. In this case, the person who is deceived can also hand over it to someone sent by the person who cheated.
3. Only in this case, because of the element of intent, this means that the element of submission must be a direct result of the efforts made by the fraudster.
4. The element of using a fake name. The use of a fake name will occur if someone mentions a name that is not their name, thereby receiving goods that must be handed over to the person whose name was mentioned earlier.
5. The element of wearing false dignity. By false dignity is meant to represent himself in a condition that is not true and which causes the victim to trust him, and based on that trust he hands over an item or gives a debt or writes off a receivable.
6. Elements of using deception and elements of a series of lies. The element of deception is a series of words, but rather from an action in such a way, that the action creates trust in other people, while a series of lies is a series of lies or words that are contrary to the truth which gives the impression that what what is said is true.

A person can only be said to have committed a criminal act of fraud as intended in Article 378 of the Criminal Code, if the elements mentioned in that article have been fulfilled, then the perpetrator of the criminal act of fraud can be punished according to his actions. Article 378 of the Criminal Code concerning criminal acts of fraud formulates, namely:

> "Whoever, with the intention of unlawfully benefiting himself or another person, by using a false name or false dignity, by means of deceit or a series of lies, induces another person to hand over something to him, or to give a debt or write off a receivable, shall be punished for fraud by a criminal offense. imprisonment for a maximum of four years".

From the formulation of Article 378 of the Criminal Code above, the elements of criminal acts of fraud, like criminal acts in general, consist of objective and subjective elements. Subjective elements include intentions to benefit oneself or others and are against the law. The objective element includes the act (moving), the act being moved (person), the act directed at another person (handing over objects, giving debts, and writing off receivables), and the method of carrying out the act of moving by using a false name, using deception, using false dignity., and uses a series of lies.

Other fraud is regulated in Article 379 of the Criminal Code which is usually referred to as a crime of light fraud. This term is used by taking into account the elements contained in the formulation of Article 379 of the Criminal Code, namely the actions described in Article 378 of the Criminal Code, if the goods provided are not livestock and the price of the goods or debt is not more than two hundred and fifty thousand rupiah, it is punished as light fraud with three months' imprisonment or a fine of fifteen times sixty rupiah. From this explanation it can be formulated that there are elements of minor criminal acts of fraud, including:

1. Elements of fraud in Article 378 of the Criminal Code.
2. The goods provided are not livestock.
3. The price of the goods, debts or receivables does not exceed two hundred and fifty rupiah.

Regulations regarding criminal acts of fraud are not only contained in the Criminal Code, because the development of society has become increasingly sophisticated and the number of modus operandi used varies, there are special regulations that regulate and formulate criminal acts of fraud in Law of the Republic of Indonesia Number 11 2008 concerning Information and Electronic Transactions. This law was then revised again in 2016 to become Law of the Republic of Indonesia Number 19 of 2016 concerning Electronic Information and Transactions.

The Information and Electronic Transactions Law has undergone two changes since it was promulgated. First, the amendment became Law of the Republic of Indonesia Number 19 of 2016 which shows the dynamics and desire of the public for improvements to the articles of the Information and Electronic Transactions Law, especially in illegal content criminal provisions. As for the second change, it emphasizes the importance of realizing justice, public order and legal certainty in society.

Law of the Republic of Indonesia Number 19 of 2016 concerning Electronic Information and Transactions discusses criminal acts committed using online networks. Starting from information, electronic transactions to prohibited things that are legally contrary to regulations carried out in cyberspace. In Law of the Republic of Indonesia Number 19 of 2016 concerning Information and Electronic Transactions there is no specific explanation regarding fraud, this can be seen from the absence of the use of the proposition 'fraud' in its articles.

There are regulations regarding the prohibition of spreading fake news which results in harm to people, namely in Article 28 Paragraph (1) of Law of the Republic of Indonesia Number 19 of 2016 concerning Information and Electronic Transactions which states that every person intentionally and without right spreads false and misleading news which resulting in consumer losses in electronic transactions.

Although this verse does not specifically explain fraud, it is very clear about the dimensions of the criminal act of fraud. In the Second Amendment to Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions, there are changes to the content of the sentences in Article 28 Paragraph (1). Article 28 Paragraph (1) states that every person intentionally distributes and/or transmits electronic information and/or electronic documents containing false notices or misleading information which results in material losses for consumers in electronic transactions.

The elements contained in Article 28 Paragraph (1) of the Information and Electronic Transactions Law are identical and have several similarities with conventional criminal acts of fraud regulated in Article 378 of the Criminal Code and have special characteristics, namely the recognition of evidence, electronic media and the expansion of jurisdiction. in the Electronic Information and Transactions Law. The relationship between Article 28 Paragraph (1) of the Information and Electronic

Transactions Law and Article 378 of the Criminal Code is seen from the elements that regulate actions related to that article.

The threat of violating Article 28 Paragraph (1) of the Information and Electronic Transactions Law can be imprisonment for a maximum of six years and/or a fine of a maximum of IDR. 1,000,000,000 (one billion rupiah) in accordance with the provisions contained in Article 45A Paragraph (1) of the Information and Electronic Transactions Law which states that every person intentionally and without right spreads false and misleading news which results in consumer losses in transactions Electronics as intended in Article 28 Paragraph (1) shall be punished with a maximum imprisonment of 6 (six) years/or a maximum fine of IDR 1,000,000,000 (one billion rupiah).

In the Second Amendment Law to Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions in Article 45A Paragraph (1), the content of the sentence also changes, namely to read every person who deliberately distributes and/or transmits electronic information and/ or electronic documents containing false notifications or misleading information which results in material losses for consumers in electronic transactions as intended in Article 28 Paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of Rp. 1,000,000,000.00 (one billion rupiah).

There are differences in two articles between the Criminal Code and the Information and Electronic Transactions Law, namely that the formulation of Article 28 Paragraph (1) of the Information and Electronic Transactions Law does not require the element of "benefiting oneself or others" as regulated in Article 378 of the Criminal Code concerning fraud. In reality, investigators can use multiple articles for a criminal act that fulfills the elements of a criminal act of fraud as regulated in Article 378 of the Criminal Code and fulfills the elements of a criminal act in Article 28 Paragraph (1). Information and Electronic Transactions Law This shows that if the elements of a criminal act are met, then investigators can use these two articles.

The emergence of Law of the Republic of Indonesia Number 19 of 2016 concerning Information and Electronic Transactions provides two important things, namely, firstly, recognition of electronic transactions and electronic documents within the framework of the law of engagement and law of evidence, so that legal certainty of electronic transactions can be guaranteed and secondly it is classified as an act. Actions that qualify as legal violations related to misuse of information technology are accompanied by criminal penalties. However, sometimes society is still in a weak position. The main factor that causes community weakness is often due to the low level of legal knowledge and awareness of their rights.

Law Enforcement Against Fraud Crimes Using Online Invitation Mode

Online fraud is a term used for internet users who experience criminal acts of fraud. Online fraud can take the form of stealing personal data, which can trigger identity theft, internet services that can be used to deceive victims or carry out fraudulent transactions. Online fraud can occur via chat, social media (social media), email, or websites.

The crime of online fraud is included in the group of illegal contents crimes in the study of misuse of information technology in the form of computer related fraud. Illegal contents is a crime involving falsifying data or information on the internet about something that is incorrect, unethical, and can be considered to violate the law or disturb public order. Computer related fraud is defined as cheating or fraud that is created to gain personal gain or to harm other people.(Aswan, 2019)

Fraud that occurs in the cyber world today can be carried out in various ways, one of which is the online invitation mode. The online invitation mode is no different from the previous method which also went viral, namely when asking the victim to install a certain application which is actually used to steal SMS OTP mobile banking services. This mode of fraud via online invitations is widely spread via the WhatsApp application. Even though it's called a wedding invitation. However, the file format sent turned out to be APK or the file format for Android applications. In the content of the message distributed, the sender did not show his identity. However, the sender only asks the recipient to open the APK file he sent to find out the information provided to the victim.

According to the Director of the Cyber Crime Directorate, the online invitation mode is relatively new and different from fraud using the Android operating system application or APK method. This mode of fraud with online invitations generally aims to gain financial gain by hacking methods, when the victim starts to get 'trapped' by opening the invitation, their smart device can be directly accessed by hackers. They can open the victim's digital banking application to mobile banking.

If they are not observant, the recipient will not know that the document being distributed is a fake invitation that is used to compromise the victim's personal data, by accessing the banking data of the owner of the number to which the invitation was sent. According to Bareskrim Polri, since the end of 2022, there have been 29 (twenty nine) reports related to cases of fraud using the online invitation mode.

Law enforcement issues, including law enforcement for criminal acts of online fraud, are a very serious problem for a country, especially in the Unitary State of the Republic of Indonesia. This problem is not a problem that is very easy to find a solution or solution to, but the problem lies in the practice of law enforcement itself.(Pawenne, n.d.)

Law enforcement can be formulated as an effort to implement the law as it should, monitor its implementation so that violations do not occur, and if a violation occurs, restore the violated law so that it is re-enforced.(Rahmanto, n.d.). Law enforcement is closely related to compliance by users and implementers of statutory regulations, in this case both the public and state administrators, namely law enforcers.(Machmud, 2012). The main aim of law enforcement is to create a sense of justice, legal certainty and benefit in society.

There are several factors in the law enforcement process that influence the success of its implementation, namely law; law enforcer; means or facilities that support law enforcement; public; and culture. Further to these factors, the law enforcement process, apart from having a set of statutory regulations, also requires a driving instrument. The driving instrument is the law enforcement institution and all its

implementation through working mechanisms in a system, namely the criminal justice system.(Indarti, n.d.)

Criminal law enforcement currently has an urgent need for fundamental changes in order to achieve the goal of better and more humane punishment. This need is in line with the strong desire to be able to realize law enforcement that is fairer towards every form of criminal law violation.(Dendi Pajriansyah, 2023) Criminal law enforcement is an effort to realize ideas about justice in criminal law in legal certainty and social benefits into legal reality in every legal relationship.

Law enforcement is a problem in almost every country, especially in developing countries. Legal problems are many and varied, both in terms of qualifications and modus operandi. There are many legal problems, many of which have not been resolved or may even be difficult to resolve. One problem that is still difficult is online fraud in cybercrime. These legal problems occur in a complex and systemic manner. Therefore, improvements must also be carried out systemically.

It is necessary to strictly enforce the law by law enforcement officials against criminal acts of fraud using the online invitation mode in order to reveal every perpetrator of criminal acts of online fraud as intended in the law. This will be a benchmark for the community regarding the performance of law enforcement officers.

It is often very difficult for law enforcement officials to differentiate between conventional fraud and online fraud, so it is up to law enforcement to determine when to use Article 378 of the Criminal Code and when to use the provisions in Article 28 Paragraph (1) of the Information and Electronic Transactions Law. However, in practice law enforcement authorities can impose multiple articles on a criminal act that fulfills the elements of a criminal act of fraud as regulated in Article 378 of the Criminal Code and fulfills the elements of a criminal act in Article 28 Paragraph (1) of the Information and Electronic Transactions Law. This means that if the elements of a criminal act are met, law enforcers can use these two articles or indeed law enforcers can file alternative charges.(Zubaidah, n.d.)

Talking about the system of proof for perpetrators of criminal acts of fraud using the online invitation mode, if you use the Criminal Procedure Code as a basis for proving this unconventional crime, it is very difficult to prove it because of the limited legal evidence according to Article 184 of the Criminal Procedure Code. To more precisely prove the guilt of someone who commits a crime in the cyber domain, a special law that can be used in this case is the Information and Electronic Transactions Law which can be used to prove someone's guilt in this proof.

To prove the guilt of a person who commits a criminal act of fraud using the online invitation mode, the more appropriate article to use is Article 5 and Article 6 of the Information and Electronic Transactions Law which is an extension of the documentary evidence and instructions in Article 184 Paragraph (1) letter (c) and (d) KUHAP.(Sitompul, 2012) Although there are limitations in electronic evidence contained in Article 5 Paragraph (4), namely letters which according to the law must be made in written form and letters and their documents which according to the law must be made in the form of a notarial deed or a deed made by the official making deed.

Law enforcement in Indonesia is currently experiencing difficulties in dealing with the spread of cyber crime. The obstacles in law enforcement are due to the fact that there are still very few law enforcement officers who understand the ins and outs of information technology (internet), limited facilities and infrastructure, and a lack of public legal awareness in efforts to overcome information technology crimes. Apart from that, law enforcement officers in the regions are not yet ready to anticipate the rise of this crime because there are still many law enforcement officers who are technologically deficient. This is because there are still many law enforcement institutions in the regions that are not yet supported by an internet network.

Law enforcement currently carried out by the Police is arresting fraud perpetrators using online invitation mode. The National Police Headquarters Cyber Team, based on the victim's report, arrested the perpetrator with the initials AI (20 years old) who works as a student from South Sulawesi. AI creates these applications and then buys and sells them and then the buyers use them to commit crimes to deceive many of their victims. In the network of perpetrators who purchased the application, one perpetrator was arrested in Sumatra and one in Wajo Regency.

In the end, to ensnare perpetrators of criminal acts of fraud using online invitation mode, the legal basis that can be given to perpetrators is Article 378 of the Criminal Code. However, Article 378 of the Criminal Code concerning criminal acts of fraud cannot be used to burden perpetrators of criminal acts of fraud using the online invitation mode to take responsibility for their actions, because there are several obstacles in imposing criminal sanctions on perpetrators of criminal acts, such as obstacles in proving where evidence is limited by the Criminal Procedure Code. Therefore, to strengthen the legal basis, Article 28 Paragraph (1) of the Electronic Information and Transactions Law can be added.

CONCLUSION

The conclusions obtained based on the results of the discussion are: The criminal act of fraud in Indonesian law is regulated in the Criminal Code and the Information and Electronic Transactions Law as a legal umbrella for electronic transaction activities and use in the field of information and communication technology. In the Criminal Code, the crime of fraud is regulated in Chapter XXV Book II of the Criminal Code Articles 378-395 and specifically regulated in Article 378 of the Criminal Code, while online fraud is regulated in Article 28 Paragraph (1) of the Information and Electronic Transactions Law. The online invitation mode for criminal fraud is relatively new. According to Bareskrim Polri, since the end of 2022, there have been 29 (twenty nine) reports related to cases of fraud using the online invitation mode. The law enforcement carried out by the Police currently against perpetrators of fraud using the online invitation mode is to make arrests, one of which is arresting the perpetrator who created the online invitation application. Law enforcers usually impose multiple articles as regulated in Article 378 of the Criminal Code and Article 28 Paragraph (1) of the Information and Electronic Transactions Law with the threat of imprisonment for a maximum of 6 (six) years and/or a maximum of Rp. 1,000,000. 000, while to prove the perpetrator's guilt, Article 5 and Article 6 of the Information and Electronic Transactions Law are used as recognition of information, documents and electronic signatures as valid evidence in court.

REFERENCES

Akangbe, Raphael. "Healthcare Data Protection in the Era of Digital Health." *Researchgate*, no. August (2022).

Amir, Nabbilah. "Legal Protection of Patient Data Confidentiality Electronic Medical Records (Perlindungan Hukum Kerahasiaan Data Pasien Dalam Rekam Medik Elektronik)." *SOEPRA Jurnal Hukum Kesehatan* 5, no. 2 (2019): 198–208. http://journal.unika.ac.id/index.php/shk198.

Aptika Kominfo. "Digitalisasi Pelayanan Kesehatan Dengan Penerapan Revolusi Industri," n.d.

———. "Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya Di Internet," n.d.

CNN Indonesia. "Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat," n.d.

Damargara, Muhammad Izzar, Muhammad Alhidayah, Muhammad Raihan Faiqy, and Jatnika Maulana. "Urgensi Realisasi Pengaturan Data Protection Officer (DPO) Pada Sektor Kesehatan Ditinjau Dari Hukum Perlindungan Data." *Padjadjaran Law Research* 10, no. 1 (2022): 38–55.

Hellmeier, Malte, and Franziska von Scherenberg. "A Delimitation of Data Sovereignty from Digital and Technological Sovereignty." *Thirty-First European Conference on Information Systems (ECIS 2023)* 1, no. June (2023).

Hs, Bambang Dwi. "Legal Aspect of Patient's Medical Record." *Advances in Economics, Business and Management Research* 121, no. Inclar 2019 (2020): 76–79. https://doi.org/10.2991/aebmr.k.200226.015.

Jain, Dipika. "Regulation of Digital Healthcare in India: Ethical and Legal Challenges." *Healthcare (Switzerland)* 11, no. 6 (2023). https://doi.org/10.3390/healthcare11060911.

Kemalasari, Ni Putu Yuliana, and I Putu Harry Suandana Putra. "Protection of Medical Record Data as a Form of Legal Protection of Health Data through the Personal Data Protection Act." *Journal of Digital Law and Policy* 2, no. 3 (2023): 111–18. https://doi.org/10.58982/jdlp.v2i3.338.

Kosegeran, Gilbert, and Dientje Rumimpunu. "Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin." *Lex Privatum* IX, no. 12 (2021): 89–98. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/38447.

Kurniawan, Alfian Listya, and Anang Setiawan. "Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19." *Jurnal Hukum Dan Pembangunan Ekonomi* 9, no. 1 (2021): 95. https://doi.org/10.20961/hpe.v9i1.52586.

Lalu Anugrah Nugraha, Sutarno Sutarno, Ninis Nugraheni, and Andika Persada Putra. "Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Peresepan Elektronik." *Unizar Law Review* 6, no. 2 (2023). https://doi.org/10.36679/ulr.v6i2.45.

Lintang, Kastania, and Yeni Triana. "Perlindungan Hukum Terhadap Hak Privasi Dan Rekam Medis Pasien Pada Masa Pandemi Covid-19 (Legal Protection Of Patients Privacy Rights And Medical Records In The Covid-19 Pandemic)." *Rewang Rencang : Jurnal Hukum Lex Generalis* 2, no. 10 (2021): 913–27.

Maria Maddalena Simamora, Indah. "Perlindungan Hukum Atas Hak Privasi Dan Kerahasiaan Identitas Penyakit Bagi Pasien Covid-19." *SIBATIK JOURNAL: Jurnal*

Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan 1, no. 7 (2022): 1089–98. https://doi.org/10.54443/sibatik.v1i7.126.

Notoatmodjo, S. *Metodologi Penelitian Kesehatan*, 2018.

Putra, Calvin Anthony. "Data Rekam Medis Elektronik Akibat Cyber Crime Calvin Anthony Putra." *Jurnal Novum* 1, no. 1 (2021): 0–216.

Putri, Ririn Noviyanti. "Indonesia Dalam Menghadapi Pandemi Covid-19" 20, no. 2 (2020): 705–9. https://doi.org/10.33087/jiubj.v20i2.1010.

Retnowati, Anny. "Politik Hukum Dalam Menata Rekam Medis Sebagai Sarana Perlindungan Hukum Terhadap Rumah Sakit, Dokter Dan Pasien." *Yustisia Jurnal Hukum* 2, no. 2 (2018). https://doi.org/10.20961/yustisia.v2i2.10208.

Simamora, Tri Putri, Sonya Airini Batubara, Indra Efrianto Napitupulu, and Robinson Tamaro Sitorus. "Perlindungan Hukum Terhadap Pasien Dalam Pelayanan Medis Di Rumah Sakit Umum." *Al-Adl : Jurnal Hukum* 12, no. 2 (2020): 270. https://doi.org/10.31602/al-adl.v12i2.3091.

Sitanggang, Tiromsi. *Aspek Hukum Kepemilikan Rekam Medis Terhadap Perlindungan Hak Pasien*. Edited by Feriyansyah. 1st ed. Medan: Yayasan Kita Menulis, 2019.

Utomo, Handryas Prasetyo, Elisatris Gultom, and Anita Afriana. "Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Teknologi Di Indonesia." *Jurnal Ilmiah Galuh Justisi* 8, no. 2 (2020): 168. https://doi.org/10.25157/justisi.v8i2.3479.

Wijaya, Yudi Yasmin, Edy Suyanto, and Fanny Tanuwijaya. "Rekam Medis: Penggunaan Informasi Medis Pasien Dalam Pelaksanaan Asas Perlindungan Publik." *Veritas et Justitia* 6, no. 2 (2020): 399–423. https://doi.org/10.25123/vej.3717.