International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

Application Of Criminal Sanctions To Perpetrators Of Crimes *Intentionally And Without Rights Against The Law Accessing Computers Or Electronic Systems Other People's Own (Study of* Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk)

Annafi Akbar[1] *
[1]University of Bandar Lampung, Indonesia
Anggalana[2]
[2]University of Bandar Lampung, Indonesia

*Corresponding Author email: annafiakbar89@gmail.com

Abstract

One of the decisions related to the criminal act of intentionally and without the right to access another person's computer or electronic system is recorded in the Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk. In this case, the Defendant VAR bin I is suspected of committing the act in the period April 2022 to December 2024 at his residence in Kupang Jernih, Sukarame II Village, West Teluk Betung District, Bandar Lampung City, or other locations that are still within the jurisdiction of the Tanjung Karang District Court. This study aims to analyze the application of criminal sanctions and the judge's considerations in imposing penalties on the perpetrator based on the decision. The research method uses a normative and empirical juridical approach with primary and secondary data, through library and field research, and is analyzed qualitatively. The results of the study indicate that the application of criminal sanctions against the defendant is based on Article 30 paragraph (1) in conjunction with Article 46 paragraph (1) of Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions and Law No. 8 of 1981 concerning Criminal Procedure Law, with a prison sentence of 9 months and a fine of Rp5,000,000,-, replaced by 3 months imprisonment if the fine is not paid. The judge's considerations include aggravating factors, namely unlawful acts, as well as mitigating factors, such as the defendant's confession, polite behavior, no previous convictions, and reconciliation with the victim. This reflects the judge's efforts to balance justice,

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

deterrent effects, and mitigating circumstances for the defendant. It is recommended that law enforcement officers and judges always consider evidence, motives, and mitigating or aggravating circumstances to ensure a fair, proportional, and legal-compliant verdict.

Keywords: Implementation; Criminal Sanctions; *Against the Law* ; Computer; Legal System.

INTRODUCTION

The crime of intentionally and without authorization accessing another person's computer or electronic system is a form of *cybercrime* that is increasingly under scrutiny in today's digital era. This act not only causes material losses to the system or data owner but can also compromise the security and integrity of electronic systems nationally. The impacts of this illegal access include data theft, disruption of electronic services, and the potential misuse of sensitive information for criminal purposes. This type of cybercrime demands serious attention from law enforcement officials, system administrators, and the public to minimize the risk of loss. Illegal access to electronic systems is not only an individual problem but also a strategic issue in national security.

Law enforcement against crimes of illegal access or hacking of electronic systems requires a thorough and accurate evidentiary process, particularly given the digital nature of these crimes. Electronic evidence, such as *server logs* , *metadata* , and access traces, must be collected legally and verified using computer forensic methods to ensure its validity and reliability in court. This process is not only crucial for enforcing the law against perpetrators but also for protecting victims' rights, including the right to personal data and information confidentiality. Furthermore, the appropriate use of forensic technology helps avoid misidentification of perpetrators and ensures that legal decisions are based on valid facts. Therefore, thorough evidentiary preparation is key to effective law enforcement in combating cybercrime.[1]

The primary normative basis for the crime of unauthorized access or interception of another person's electronic information is contained in Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) and its amendments. This law explicitly criminalizes hacking, illegal access, and interception of electronic data, thus providing law enforcement with the legal framework to prosecute perpetrators. The law enforcement process can be carried out clearly, including in terms of evidence and the imposition of criminal sanctions. Besides being a repressive instrument, this regulation also serves a preventative function to

[1]Bambang Hartono. 2013. *Application of Criminal Sanctions to Carding Crimes* , Jurnal Pranata Hukum, Vol. 8, No. 2, 2013, pp. 141-156.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

prevent hacking and unauthorized access to electronic systems. The ITE Law stipulates that anyone who intentionally and without authority accesses another person's electronic system can be punished, thus providing legal protection for data owners.[2]

The main elements of the crime of unauthorized access consist of (a) the act of accessing or entering another person's system/computer; (b) done intentionally; and (c) without rights or exceeding authority. In law enforcement practice, proving these elements requires technical examination (logs, digital forensics) and proof of the perpetrator's intent so that the elements of *mens rea* and *actus reus* can be fulfilled in a criminal verdict. Empirical studies emphasize the importance of digital evidence that maintains the chain of evidence so that criminal charges can be maintained in court.[3]

Criminal sanctions for unauthorized access vary, ranging from imprisonment to fines, depending on the provisions of the alleged article and the resulting consequences (e.g., data loss, alteration, or transfer). In addition to the ITE Law, developments in data security and protection regulations also influence the choice of articles prosecutors use when prosecuting, for example, if the act results in loss of personal data or service disruption. Sanctions applied should not only consider the act of access itself but also its concrete impact on the victim and infrastructure.[4]

In criminal justice practice, judges and prosecutors face both technical and normative challenges: first, determining the qualifications of an act (whether it truly constitutes "unauthorized access" or simply an abuse of granted access), and second, assessing the causal relationship between the unauthorized access and the claimed harm. Books and articles on cyber law emphasize the need for standard digital forensic evidence guidelines and increased investigator capacity to ensure proportionate and accountable sanctions.

A preventative perspective and criminal policy considerations suggest that criminal sanctions must be balanced with administrative and civil remedies, such as data recovery, security remediation orders, and compensation. The new personal data protection law also adds a dimension of administrative sanctions and *civil remedies* that can run parallel to criminal proceedings. Therefore, modern law enforcement against unauthorized access often involves a

[2]Adhisti Syifani Pasaribu and Anggalana. 2024. *Legal Review of Electronic Information and Transactions that Intentionally and Without Rights Transmit Electronic Information and/or Electronic Documents Containing Moral Content* , Jalakotek: Journal of Accounting Law Communication and Technology, Vol. 1, No. 2, July 2024, pp. 205-209.

[3] Ibrahim Fikma Edrisy. 2019. *Introduction to Cyber Law* , Sai Wawai Publishing, Metro, p. 56.

[4] MZ Husamuddin, Sumardi Efendi, Syaibatul Hamdi and Ida Rahma. 2024. *Criminal Procedure and Cyber Crime* , PT Media Penerbit Indonesia, North Sumatra, p. 77.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

combination of criminal sanctions, administrative fines, and civil action.[5]

When sentencing, courts need to consider aggravating and mitigating factors: economic or commercial motives, the scale and nature of the damage (e.g., *ransomware that encrypts data), ties to organized cybercrime, and whether the perpetrator cooperated and made restitution. Contemporary cases (including ransomware* incidents) demonstrate that crimes involving data locking and extortion tend to be viewed as more serious and can lead to heightened criminal penalties.[6]

In addition to the primary penalty (imprisonment/fines), the practice of imposing sanctions can include additional sanctions such as mandatory restitution/compensation, prohibition of access/employment in certain fields, or mandatory participation in IT skills rehabilitation programs. This approach, which combines punitive and remedial effects, can reduce the residual risk of reoffending *and* assist victims' recovery. The application of criminal sanctions to perpetrators who intentionally and without authority access computers or electronic systems belonging to others must be based on a clear legal basis, strong forensic evidence, and consideration of proportionality in the context of the real impact on the victim. Regulatory reform and increasing the capacity of law enforcement are prerequisites for criminal sanctions to be effective, fair, and capable of creating a deterrent effect without sacrificing legal certainty.

One of the decisions related to the crime of *intentionally and without unlawful rights to access another person's computer or electronic system is in the* Tanjung Karang District Court Decision Number 596 / Pid.Sus / 2025 / PN Tjk. Based on the results of the trial, the Panel of Judges stated that the Defendant VAR bin I on a day in April 2022 to December 2024 at the defendant's house located at Kupang Jernih LK.5 RT / RW 001 / 000 Kel. Sukarame II, Teluk Betung Barat District, Bandar Lampung City or at least in another place that is still included in the jurisdiction of the Tanjung Karang District Court. The defendant was legally and convincingly proven guilty of committing a crime *by intentionally and without unlawful rights to access another person's computer and / or electronic system in any way* as regulated in the third indictment. the defendant installed illegal access on *the server* belonging to CV. The Aero Global Security System has 191 *GPS trackers* so that the victim, namely witness Deasy Syafarina as the owner of the Aero Security System shop under the auspices of CV. Aero Global Security System, suffered a loss of Rp.

[5]Risman Hi Mustafa, Mulyati Pawennai and Mursyid **.** 2020. *Hacking of Electronic Systems in Public Transportation Applications* , *Qawanin Journal of Legal Studies* , Vol. 1, No. 1, 2020, pp. 59–71.

[6] Inggou David Purba. 2024. *The Criminal Offense of Illegal Access (Hacking) to Computers or Electronic Systems* , *Bulletin of Community Engagement* , Vol. 4, No. 2, 2024, pp. 440-458.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

191,000,000,- (one hundred and ninety-one million rupiah). On this basis, the Panel of Judges sentenced the Defendant to 9 (nine) months in prison **and** a fine of Rp. 5,000,000,- (five million rupiah) , with the provision that if the fine is not paid, it will be replaced with 3 (three) months in prison. In addition, the Panel of Judges determined that the period of arrest and detention that the Defendant has served is deducted entirely from the sentence imposed.

The urgency of implementing criminal sanctions against perpetrators of criminal acts who intentionally and without legal authority access other people's computers or electronic systems is very important in the context of modern law enforcement, considering the rapid development of information technology and the increasing number of cybercrime cases that harm individuals and institutions. The study of Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk provides an opportunity to evaluate the effectiveness of the application of articles in the Electronic Information and Transactions Law (UU ITE), especially in upholding the principles of justice and legal certainty. This research is also important to understand the extent to which criminal sanctions, whether in the form of imprisonment or fines, are able to provide a deterrent effect, protect victims' rights, and encourage legal compliance in the digital realm.

METHOD

This research uses a normative and empirical juridical approach to obtain a comprehensive understanding of the legal issues studied. The data used include primary data, in the form of direct information from relevant sources through interviews or field observations, as well as secondary data obtained from documents, laws and regulations, court decisions, and other relevant literature. Data collection was conducted through library research to examine written legal materials and field research to obtain direct empirical data. Data analysis was conducted qualitatively by interpreting, reviewing, and connecting the information obtained to answer the research problem formulation in depth and systematically.

DISCUSSION

Implementation of Criminal Sanctions Against Criminals Who Intentionally and Without Rights Against the Law Access Computers or Electronic Systems Belonging to Others Based on Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk

The crime of intentionally and without legal authority to access another person's computer or electronic system is an act committed by a person with the intent to enter, use, or retrieve data from an electronic system without the owner's permission. This act falls under the category of

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

cybercrime as regulated by the Electronic Information and Transactions Law. This act can take the form of data theft, system destruction, or alteration of information to the detriment of another party. The essence of this crime is the intentional violation of legal access rights. This crime can result in material and immaterial losses for the victim. Therefore, any illegal access to an electronic system is subject to criminal sanctions in accordance with applicable law.

The imposition of criminal sanctions against perpetrators of this crime is based on the principle of justice and clear legal considerations. Perpetrators can be subject to imprisonment and/or fines in accordance with the provisions of Articles 30 and 46 of the ITE Law. In practice, judges consider aggravating and mitigating factors, including the extent of the harm caused and the defendant's demeanor during the trial. Criminal sanctions aim to provide a deterrent effect and protect the public from similar actions. Furthermore, the imposition of sanctions also encourages legal awareness among users of electronic systems. Thus, law enforcement against cybercrime is a crucial instrument in maintaining digital security.

Based on interviews with Bandar Lampung Police investigators, handling of illegal computer access cases always begins with an investigation to verify digital evidence. Investigators emphasize the importance of log documents and expert witnesses in strengthening the case. Cases that harm other parties will be prioritized for follow-up according to legal procedures. Investigators also consider the perpetrator's intent and deliberateness in committing the act. In Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk, the perpetrator was proven to have accessed without authorization and was subject to criminal sanctions. This demonstrates the police's seriousness in enforcing the law in the cyber realm.

Interviews revealed that the police emphasize evidence and the perpetrator's intent as key elements in the investigation process. Digital evidence and expert witnesses are crucial elements in strengthening criminal charges. The emphasis on intent demonstrates that not all illegal access is criminally punishable; unlawful intent must be proven. Investigators also demonstrated good coordination with the prosecutor's office to ensure smooth prosecution. This analysis confirms that investigative procedures are not merely technical but also consider aspects of justice for both victims and defendants. This, in turn, contributes to more systematic and transparent cyber law enforcement.

Prosecutors at the Bandar Lampung District Attorney's Office explained that the prosecution of the perpetrator of illegal computer access was based on evidence from the police investigation. They emphasized the importance of verifying digital documents and expert witness testimony before indicting. In Tanjung Karang District Court Decision No. 596/Pid.Sus/2025/PN

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Tjk, prosecutors successfully proved the perpetrator's intent and deliberate actions. Prosecutors also considered aggravating and mitigating factors in drafting criminal charges. The goal is to provide a deterrent effect while upholding justice for the victim. This reflects the importance of cybercrime prosecutions and adherence to legal procedures.

Interviews revealed that prosecutors play a crucial role in ensuring that digital evidence and expert testimony are thoroughly reviewed before prosecution. Emphasis on the perpetrator's intent reinforces the principle that sanctions only apply to deliberate and unlawful acts. Prosecutors also balance deterrence and justice for both the defendant and the victim. This process demonstrates strong coordination between investigators and prosecutors. This analysis confirms that prosecuting cybercrime cases requires high levels of professionalism and precision, leading to more accurate and effective law enforcement against cybercrime.

Based on an interview with the judge at the Tanjung Karang District Court, the application of criminal sanctions against perpetrators of criminal acts who intentionally and without legal rights access another person's computer or electronic system refers to Decision Number 596/Pid.Sus/2025/PN Tjk. The sanctions are given based on Article 30 paragraph (1) in conjunction with Article 46 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 8 of 1981 concerning Criminal Procedure Law. The perpetrator was sentenced to 9 (nine) months in prison and a fine of IDR 5,000,000 (five million rupiah), with the provision that if the fine is not paid, it will be replaced with 3 (three) months in prison. The judge explained that legal considerations also include aggravating and mitigating circumstances, such as the defendant's confession and reconciliation with the victim. The trial process was carried out transparently to ensure justice and compliance with legal procedures. This demonstrates the proportional application of the law and is in accordance with laws and regulations related to cybercrime.

Based on the research results, it can be analyzed that the imposition of criminal sanctions on perpetrators emphasizes the principles of proportionality and compliance with statutory regulations. Imprisonment and fines demonstrate a combination of deterrent effects and legal protection for victims. The provision of replacing fines with imprisonment emphasizes legal certainty in the application of sanctions. The defendant's confession and reconciliation with the victim are mitigating factors, ensuring a just and humane sentence. This analysis confirms that the judge in the Tanjung Karang District Court's decision firmly enforced the Electronic Information and Transactions (ITE) law while still adhering to the principle of justice. The application of criminal sanctions in cases of illegal computer access is both educational and deterrent for the community.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Based on the research results, it can be analyzed that the application of criminal sanctions against perpetrators of criminal acts who intentionally and without legal rights access computers or electronic systems belonging to other people based on the Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk based on Article 30 paragraph (1) Jo Article 46 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and Law Number 8 of 1981 concerning Criminal Procedure Law and other relevant laws and regulations with a prison sentence of 9 (nine) years and a fine of IDR 5,000,000 (five million rupiah) with the provision that if the said criminal fine is not paid it will be replaced with imprisonment for 3 (three) months.

Considerations in Sentencing Criminals Who Intentionally *and Without Rights Against the Law Access to Computers or Electronic Systems Belonging to Other People Based on* Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk

Judicial deliberation is the analytical and evaluation process undertaken by a judge before handing down a criminal sentence to a defendant. This process includes examining facts, evidence, and witness or expert testimony related to the case. Judicial deliberation also takes into account legal, moral, and social aspects to ensure a fair and proportionate verdict. In addition, the judge assesses the defendant's aggravating and mitigating circumstances. The purpose of these deliberations is to balance the interests of the victim, the defendant, and the community. Judicial deliberation is the primary basis for imposing criminal sanctions.

The judge's considerations in sentencing a perpetrator of a crime of intentionally and without legal authority to access another person's computer or electronic system involve an analysis of the evidence and the defendant's intent. Aggravating circumstances are those in which the defendant's actions are clearly unlawful and detrimental to the victim. Meanwhile, mitigating circumstances include the defendant's confession, polite behavior during the trial, no previous convictions, and a reconciliation with the victim. The judge considers this combination of factors necessary to impose a proportionate sentence. This consideration also aims to provide a deterrent effect while still taking into account humanitarian values. The decision must balance justice and legal certainty.

Based on interviews with Bandar Lampung Police investigators, the judge carefully considered digital evidence and expert witnesses before sentencing. Investigators explained that the defendant's intent and deliberate actions were the primary focus of the judge's deliberations. Aggravating circumstances, such as the losses incurred, were also taken into account in the

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

verdict. Mitigating factors, including the defendant's confession and reconciliation with the victim, were also taken into consideration. According to investigators, this demonstrates the judge's effort to balance deterrence with justice for the defendant. This process reflects a fair and systematic application of legal principles.

The interview results above indicate that the judge's considerations are not solely based on formal evidence, but also consider aspects of intent, deliberate action, and the victim's losses. Aggravating and mitigating circumstances determine the severity of the sentence imposed. This confirms that the judge strives to create a proportional and balanced decision. Investigators believe this deliberation process increases transparency and accountability in law enforcement. It also demonstrates the importance of coordination between investigators and the court to strengthen the judicial process, as the judge's considerations reflect the principles of justice and legal certainty.

The prosecutor explained that the judge, in imposing the sentence, considered the evidence from the investigation and the carefully prepared indictment. The defendant's intent and deliberate actions were the primary considerations in determining guilt. Aggravating circumstances, such as unlawful acts, and mitigating circumstances, including the defendant's confession and the achievement of reconciliation with the victim, were used as the basis for the verdict. The prosecutor emphasized that these considerations aimed to produce a just sentence and provide a deterrent effect. The transparent trial process allowed the judge to consider all factors proportionally. The judge's considerations demonstrated a balance between law enforcement and humanitarian values.

The interview results showed that the judge balanced formal legal aspects with humanitarian factors when sentencing. Aggravating and mitigating factors were the basis for determining the type and length of the sentence. This demonstrates that the decision is not solely about punishment but also considers justice for the defendant and the victim. The prosecutor believes that this consideration emphasizes transparency and legal certainty in the judicial process, demonstrating the importance of coordination between prosecutors, investigators, and the court. The judge's considerations can result in proportional and educational decisions.

Based on interviews with the judge, the considerations in sentencing the perpetrator of the crime of intentionally and without unlawful access to a computer or electronic system refer to the Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk. The aggravating circumstance is the defendant's clearly unlawful actions, while mitigating circumstances include the defendant's confession, polite behavior during the trial, no previous convictions, and the

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

achievement of reconciliation with the victim. The sentence imposed is 9 months imprisonment and a fine of Rp 5,000,000, with a provision for a substitute of 3 months imprisonment if the fine is not paid. The judge emphasized that this consideration balances the principles of justice, deterrent effect, and mitigating circumstances for the defendant. The trial process was conducted transparently to ensure compliance with laws and regulations. This reflects the application of the principle of proportionality in cybercrime law.

Based on the interview results, it can be analyzed that the judge's considerations emphasize a balance between the deterrent effect, justice for the victim, and mitigating circumstances for the defendant. Aggravating and mitigating considerations form the basis for determining prison sentences and fines. The provision substituting fines for imprisonment confirms legal certainty for the defendant. The judge upholds the principles of proportionality and transparency in his decision. A fair trial process strengthens public trust in the justice system. The judge's considerations not only uphold the law but also consider humanitarian and educational values for the perpetrator.

Based on the research results, it can be analyzed that the judge's consideration in sentencing the perpetrator of a criminal act who intentionally and without legal authority accessed another person's computer or electronic system based on Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk is based on several circumstances. The aggravating circumstances in this case are the defendant's actions which clearly violated the law by accessing another person's computer or electronic system without authority, thereby causing harm to the victim and disrupting the security of the electronic system in question. On the other hand, there are several mitigating circumstances, including the defendant honestly admitting his actions before the court, being polite and cooperative during the legal process, having never been convicted before thus indicating a clean criminal record, and there has been a peace and agreement with the victim. These considerations show that the judge does not solely assess the defendant's actions from the perspective of legal violations, but also pays attention to humanitarian factors and the defendant's efforts to correct his mistakes. By considering both aggravating and mitigating circumstances, the judge strives to impose a proportional, balanced, and fair sentence. This step simultaneously provides a deterrent effect so that similar actions are not repeated, but still pays attention to opportunities for social rehabilitation for the defendant. Therefore, the verdict reflects a balance between law enforcement, victim protection, and justice for the perpetrator.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

CONCLUSION

1. The application of criminal sanctions against perpetrators of criminal acts who intentionally and without legal rights access computers or electronic systems belonging to other people based on the Decision of the Tanjung Karang District Court Number 596/Pid.Sus/2025/PN Tjk based on Article 30 paragraph (1) Jo Article 46 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and Law Number 8 of 1981 concerning Criminal Procedure Law and other relevant laws and regulations with a prison sentence of 9 (nine) years and a fine of IDR 5,000,000 (five million rupiah) with the provision that if the said criminal fine is not paid it will be replaced with a prison sentence of 3 (three) months.
2. The judge's considerations in sentencing a criminal who intentionally and without legal authority accesses another person's computer or electronic system based on Tanjung Karang District Court Decision Number 596/Pid.Sus/2025/PN Tjk are based on several factors. Aggravating circumstances are the defendant's actions that are clearly against the law, while mitigating circumstances include the defendant admitting his actions, being polite during the trial, having no previous convictions, and a reconciliation between the defendant and the victim. These considerations demonstrate the judge's efforts to balance the principles of justice, the deterrent effect, and mitigating circumstances for the defendant.

SUGGESTION

1. For law enforcement officers, it is recommended to continue enforcing the application of criminal sanctions in accordance with the provisions of the ITE Law and criminal procedure law, by considering evidence, motives, and mitigating or aggravating circumstances so that decisions can reflect justice and have a deterrent effect on perpetrators of criminal acts.
2. For judges, it is recommended to always carefully consider aggravating and mitigating circumstances, including the defendant's confession, attitude during the trial, the defendant's legal record, and efforts to reconcile with the victim, so that the verdict handed down remains fair, proportional, and in accordance with applicable legal principles.

BIBLIOGRAPHY

Adhisti Syifani Pasaribu and Anggalana. 2024. Legal Review of Electronic Information and Transactions that Intentionally and Without Rights Transmit Electronic Information and/or

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Electronic Documents Containing Moral Content , Jalakotek: Journal of Accounting Law Communication and Technology, Vol. 1, No. 2, July 2024.

Bambang Hartono. 2013. Application of Criminal Sanctions for Carding Crimes , Jurnal Pranata Hukum, Vol. 8, No. 2, 2013.

Ibrahim Fikma Edrisy. 2019. *Introduction to Cyber Law* , Sai Wawai Publishing, Metro.

Inggou David Purba. 2024. The Criminal Offense of Illegal Access (Hacking) to Computers or Electronic Systems , *Bulletin of Community Engagement* , Vol. 4, No. 2, 2024.

MZ Husamuddin, Sumardi Efendi, Syaibatul Hamdi and Ida Rahma. 2024. *Criminal Procedure and Cyber Crime* , PT Media Penerbit Indonesia, North Sumatra.

Risman Hi Mustafa, Mulyati Pawennai and Mursyid. 2020. Hacking of Electronic Systems in Public Transportation Applications , *Qawanin Journal of Legal Studies* , Vol. 1, No. 1, 2020.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License