pISSN 2798-2106 eISSN 2808-4470

Studi Ilmu Sosial Indonesia
Vol. 3, No. 2, 277-308

Legal Violation Patterns in Digital Technology on Liability and Proof

Hermawan Sutanto, Rio Saputra, Didit Darmawan

Universitas Sunan Giri Surabaya

correspondence: dr.riosaputra@gmail.com

Abstract

This article explains how digital technology reshapes patterns of legal violations by altering forms of conduct, routes of accountability, and evidentiary reasoning. Digital environments enable actions through data, access credentials, and mediated communication, allowing misconduct to occur without physical presence while extending reach across jurisdictions. Violations often rely on deception, identity misuse, unauthorized access, and reputational attacks amplified by rapid replication and coordinated sharing. These characteristics complicate attribution because conduct may involve users, service providers, and layered infrastructures. The discussion proposes a normative framework that distinguishes responsibility according to control, knowledge, and causal contribution, while preserving core legal principles of legality, fault, fairness, and proportionality. It also highlights the centrality of electronic evidence, stressing integrity, verification, and lawful acquisition to prevent wrongful inference and to protect procedural rights. By clarifying how conduct, responsibility, and proof interact in digital environments, the article supports coherent legal reasoning for contemporary violations and guides policy choices that balance public safety, individual rights, and institutional duties.

Keywords: digital technology, legal violations, electronic evidence, liability, privacy, deception, platform governance.

Sutanto, H., R. Saputra, & D. Darmawan. 2023. Legal Violation Patterns in Digital Technology on Liability and Proof, Studi Ilmu Sosial Indonesia, 3(2), 277-308.

Introduction

The development of digital technology has transformed how humans communicate, work, transact, and form social networks. This change carries normative consequences for how people understand the boundaries of propriety, private space, and legal responsibility for actions performed through devices and networks. Activities that previously occurred in physical spaces now take place through platforms that facilitate the replication of information, the amplification of opinions, and the rapid circulation of content. In the digital space, an individual's actions are often perceived as trivial because they are performed without face-to-face interaction, even though their traces can remain permanent, be copied, and spread across jurisdictions. These circumstances give rise to a new need to reinterpret the relationship between actions, legal consequences, and evidence. At the same time, digital technology shapes interaction patterns that emphasize speed and connectivity, which can weaken the consideration of due care (Kolesov, 2021). Therefore, digital-based social change demands a scientific understanding of how legal violations can take on new forms, as well as how old categories of violations acquire new ways of being committed.

Digital technology also shifts the boundary between personal activities and activities that have public consequences (Loeckx, 2016). Brief posts, comments, and the distribution of audiovisual material can affect a person's reputation, sense of security, and honor, even when performed from a private space. In social practice, many digital actions are normalized as part of daily habits, leading individuals to less frequently realize that legal norms still operate over those acts. The affordability of devices, relative anonymity, and the ease of creating new accounts can lower the psychological barriers to committing infringing acts. Furthermore, platform architecture often encourages certain behaviors through interface design, sharing features, and recommendation systems, which can facilitate the spread of problematic content. This situation raises questions about the relationship between individual will and the influence of the digital environment on the choice of action. This underscores the importance of professional integrity in maintaining justice amidst continuously evolving legal dynamics (Saktiawan et al., 2021). Within a legal

framework, these changes in interaction patterns demand a careful interpretation of the elements of fault, liability, and the limits of freedom of expression. Thus, digital technology opens a new space for the reformulation of how legal violations are viewed as social practices occurring through a new medium.

The widespread circulation of digital information also alters the character of violations related to fake news, hate speech, fraud, and privacy breaches. Information can be produced and disseminated by many parties without adequate verification procedures, while recipients often process it through emotions, group identities, and personal preferences (Zimdars & McLeod, 2020). This condition is exacerbated by the dynamics of disinformation spread within a public sphere that is increasingly vulnerable to various information disruptions (Sinambela, 2022). In such circumstances, factual errors can transform into acts with legal consequences when committed with specific intent or when they cause harm to other parties. On the other hand, victims of digital violations can suffer real losses even though the perpetrator is not physically present. The repetition, recapturing, and redistribution of content can prolong a victim's suffering and expand the scope of the harm. This characteristic challenges how the law measures recovery and the proportionality of imposing sanctions. At the same time, society often judges digital acts through rapidly changing popular morality, which can widen the gap between social assessment and legal qualification. This situation highlights the need to elaborate on how digital technology directs changes in the patterns of legal violations normatively and systematically.

Digital technology also creates forms of violations related to data and identity (Rakhmanova & Pinkevich, 2020). Personal data has become a resource with economic and political value, such that its access, processing, and distribution can trigger violations of individual rights. The need for legal protection guarantees in digital interactions is becoming increasingly crucial for user security (Negara & Darmawan, 2023). Digital identities can be forged, hijacked, or manipulated to obtain profit, deceive others, or damage reputations. Identity-based crimes demonstrate that legal violations now frequently operate through representation rather than direct presence. This makes it difficult for victims to immediately identify perpetrators, while also raising questions about reasonable standards of

due care for users. The risks of electronic transaction misuse necessitate an adequate legal protection framework (Oriento et al., 2023). At the organizational level, weak data management can open opportunities for leaks or misuse, which then potentially lead to legal liability. The transformation of regulations in technology-based health services is also an essential part of maintaining public safety (Sasmita et al., 2023). In the digital space, the boundary between the primary perpetrator and the facilitating party can become blurred, as actions can occur through a chain of services, software, and platform providers. Consequently, the discussion of legal violation patterns needs to position technology as a medium that shapes the possibility of action, while simultaneously demanding firm norms to protect rights and public interests.

The change in patterns of legal violations through digital technology is also evident in the shift in evidentiary methods and the perception of truth. Electronic evidence, digital footprints, and communication recordings open new opportunities for law enforcement, yet they also create space for disputes regarding authenticity, integrity, and the methods of evidence acquisition (Ivanov et al., 2021). The validity of electronic evidence serves as the primary foundation for ensuring effective law enforcement in digital transactions (Sulaiman et al., 2023). On one hand, digital footprints can provide strong traceability. On the other hand, content manipulation, the use of anonymizing devices, and the production of synthetic materials can obscure facts. In social practice, the abundance of information can lead to attention fatigue, causing people to tend toward believing the narratives that appear most frequently or align best with their initial beliefs. This condition can influence infringing behavior, for instance, by relying on the assumption that actions will be difficult to trace or will be obscured by the noise of information. At the same time, law enforcement officials are required to understand the technical and social dynamics accompanying electronic evidence. Strong law enforcement is necessary to respond to various forms of violations in professional services based on operational standards (Safitri et al., 2023). Thus, digital technology gives rise to a normative need to organize the relationship between items of evidence, privacy rights, and due process, so that law enforcement remains fair while staying responsive to changing patterns of violations.

The prominent issue within this topic is the imbalance between the acceleration of technological innovation and the ability of legal norms to maintain certainty and justice. When the medium of action changes, elements of unlawful acts can manifest in forms that are more dispersed, layered, and involve multiple actors. Some actions appear as ordinary activities, yet normatively they can fulfill the elements of a violation because they contain fraud, hacking, extortion, or the dissemination of prohibited material. Innovation in digital-based financial services demands the strengthening of more accountable managerial governance (Putra et al., 2023). When legal norms are not adequately understood by users, repeated actions can form habits that deviate from legal standards. On the other hand, when legal norms are formulated too generally, there is a risk of varied interpretations that can disrupt the sense of justice. The optimization of the principles of healthy business competition serves as an important instrument in realizing a fair economy in the digital era (Wibowo, Darmawan, Halizah, & Mardikaningsih, 2023). This tension is also visible in the relationship between freedom of expression and the protection of honor, public order, and privacy rights. Without conceptual clarity, efforts to assess changes in legal violation patterns may fall into simplifications that ignore the character of the digital medium and the accompanying social relations.

Another problem relates to the distribution of responsibility among individuals, platform providers, and digital system managers. In many events, violations occur through facilities provided by the platform, raising questions about the boundaries of the duty of prevention, moderation, and security. The development of risk mitigation strategies on digital platforms is a crucial aspect of fulfilling legal responsibilities (Sahid et al., 2023). If responsibility is placed entirely on the individual, then aspects of system design that encourage risky behavior may be ignored. If responsibility is broadly imposed on platform providers, then issues arise concerning proportionality, control capabilities, and the potential for excessive restrictions on user freedom. Furthermore, cross-border territories in the digital space complicate accountability, as perpetrators, victims, and service providers may reside in different jurisdictions. This jurisdictional challenge also covers administrative aspects such as the application of taxes in the digital economic system (Wibowo, Darmawan,

Negara, & Hardyansah, 2023). These circumstances give rise to enforcement problems related to coordination, standard procedures, and the protection of rights. On a normative level, these issues demand a careful arrangement regarding who should be held accountable, on what basis, and within what limits, so that the changing patterns of legal violations can be understood coherently.

This study will build a conceptual understanding of the changes in legal violation patterns influenced by digital technology, so that the discussion does not stop at a list of events or narrow classifications. Normative writing based on written sources can construct a framework that explains the relationship between the digital medium, user behavior, platform structures, and the way the law assesses actions. Such a framework is essential for evaluating the adequacy of normative formulations, consistency of interpretation, and the principles of rights protection that must be maintained in law enforcement. At the policy level, this understanding helps clarify the limits of justifiable restrictions and the protection that must be provided to victims of digital violations. At the enforcement level, conceptual descriptions can enrich perspectives on electronic evidence, liability, and the proportionality of sanctions. At the societal level, scientific writing can clarify that digital behavior is part of a legal life that demands awareness of the consequences of actions. Therefore, the urgency of this study concerns certainty, justice, and order in the digital space.

The formulation of the problem in this writing is as follows: how digital technology shapes changes in legal violation patterns through shifts in the forms of actions, liability relations, and evidentiary methods in law enforcement. This question is directed at capturing the mechanism of pattern formation, rather than merely naming types of violations. The focus includes changes in the character of actions that can occur across space, across time, and through system intermediaries. The focus also includes how accountability is understood when actions involve users, platforms, and digital infrastructure. Additionally, this question includes how evidence acquires a central role because electronic evidence and digital footprints become the primary means for assessing the truth of events. With this formulation, the writing is expected to be able to construct a sharp and focused description of the relationship between

technology and changing patterns of violations, while maintaining normative precision regarding relevant legal principles.

The objective of this writing is to formulate a conceptual explanation regarding the changes in legal violation patterns shaped by digital technology, focusing on shifts in the forms of actions, responsibility, and evidence. The description is directed at constructing explanatory categories that can be used to assess the adequacy of norms and the coherence of interpretation in law enforcement. Theoretically, this writing provides a framework for understanding how the digital medium influences the relationship between actions and legal qualifications. Practically, this writing can serve as a conceptual reference for drafting enforcement guidelines, strengthening digital legal literacy, and formulating policies that maintain a balance between the protection of rights and public interests. This objective binds the entire discussion to remain focused on the mechanisms of pattern change, rather than on the description of cases.

Method

This research utilizes a qualitative literature study to build a normative framework regarding the relationship between digital technology and changes in patterns of legal violations. The primary sources consist of methodology books, legal texts, scholarly articles, and policy documents relevant to criminal law, cyber law, electronic evidence, and liability theory. The selection of sources was conducted through thematic searching that emphasizes conceptual clarity and argumentative consistency, subsequently filtered based on suitability with the problem formulation. Henn et al. (2005) is used as a reference to emphasize the need for directed question formulation, the selection of accountable materials, and the construction of a coherent argumentative flow in social research. In this study, empirical data is not utilized; thus, the strength of the research is placed on the precision of definitions, the orderliness of reasoning, and a conceptual synthesis that can be tested through cross-source comparison.

The processing of materials was carried out through systematic reading and thematic coding to highlight key concepts explaining changes in legal violation patterns, such as shifts in modes of action, technological

intermediaries, the distribution of responsibility, and the standing of electronic evidence. Each theme is broken down into sub-themes to reveal the relationships between concepts and normative points of tension for example, between freedom of expression and the protection of rights, or between privacy and enforcement needs. Bailey (2008) serves as a reference for maintaining methodological discipline in organizing materials, avoiding leaps in reasoning, and placing generalizations within reasonable limits according to the character of written sources. During the synthesis stage, aligned ideas are woven into propositions, while differing views are positioned as spaces for conceptual clarification, ensuring the discussion does not lapse into simplistic conclusions.

The normative legal research framework is employed to assess the alignment between legal principles, the formulation of norms, and the implications of interpretation regarding liability and evidence in the digital space. Diantha (2016) is used to guide the justification of legal theory, including the affirmation of legal materials, methods of normative reasoning, and the construction of arguments oriented toward certainty and justice. Validity is maintained through consistency of terminology, clarity in the scope of discussion, and a direct link between the problem formulation, themes, and conclusions. Since this research is normative in nature, critical assessment is placed on argumentative coherence and conceptual rigor, including caution in establishing categories that explain changes in patterns of legal violations without relying on quantitative claims. With this design, the method provides an adequate foundation to answer the problem formulation through an orderly synthesis of written sources.

Result and Discussion

The digital space has become a venue for various violations that take on new forms while simultaneously modifying old ones (Handoko, 2017). One prominent type is the violation of privacy and personal data, where the access, collection, dissemination, or use of data without consent occurs through mass collection mechanisms or hacking. The effectiveness of personal data protection regulations is crucial, especially in the financial technology sector, to prevent the misuse of sensitive information (Aziz et al., 2023). Such violations can take the form of using data for commercial

profiling that harms individuals or sensitive data leaks resulting from the negligence of system managers. The impact extends beyond economic loss as it touches upon personal dignity and freedom, as well as potentially leading to discrimination. Because the digital medium allows for rapid replication and wide distribution, damage starting from a single point can evolve into a systemic violation that is difficult to reverse.

Cyber fraud is another type of violation that utilizes electronic representation and communication to obtain fraudulent gains (Hamid, 2023). Modalities include phishing, online trading fraud, fake investment schemes, and the use of false digital identities to gain access to accounts or specific rights. In the context of electronic commerce, consumer protection and platform responsibility become vital to ensure smooth transaction processes and dispute resolution (Anugroh et al., 2023). The digital character facilitates the creation of disguises and social engineering, such that victims are often influenced by false trust built through technological interfaces. Economic losses that emerge quickly are often accompanied by evidence trails scattered across various services and jurisdictions, making recovery and prosecution efforts require complex technical and legal cooperation.

Attacks against the integrity of information systems and infrastructure also emerge as a form of violation with the potential to disrupt public and private functions (Hamid, 2023). Acts of system destruction through malware, ransomware, distributed denial of service, and the exploitation of software vulnerabilities can paralyze basic services such as banking, health, or logistics. Beyond material losses, such attacks pose a threat to public safety when critical services are disrupted. Crimes against information systems often demand in-depth technical analysis to link perpetrators with the resulting consequences and to determine the level of culpability as well as elements of *dolus* or negligence.

Attacks against the integrity of information systems and infrastructure also emerge as a form of violation with the potential to disrupt public and private functions (Hamid, 2023). Acts of system destruction through malware, ransomware, distributed denial of service, and the exploitation of software vulnerabilities can paralyze basic services such as banking, health, or logistics. Beyond material losses, such attacks pose a threat to public safety when critical services are disrupted. Crimes

against information systems often demand in-depth technical analysis to link perpetrators with the resulting consequences and to determine the level of culpability as well as elements of *dolus* or negligence.

Violations against honor and reputation in the digital realm take the form of hate speech, defamation through fake content, the spread of slander, and online sexual harassment. The digital space provides a platform for the amplification of damaging messages so that the effects of stigma and trauma can spread rapidly. Changes in online communication patterns and the dynamics of virtual communities significantly influence how individuals interact while potentially triggering social conflict (Darmawan, 2021). The public and persistently available character of online content prolongs the victim's period of suffering and complicates efforts for correction or reputation rehabilitation. The utilization of social media also contributes to the development of digital literature among the younger generation, which requires supervision against negative content (Kurniawan et al., 2021). Legal evaluation of such acts requires a balancing assessment between freedom of expression and the protection of personal rights, as well as attention to effective remedial mechanisms.

Violations of intellectual property rights and trade regulations have also changed face in the digital era. Content piracy, illegal software distribution, trading of counterfeit goods through online platforms, and license and patent infringements have become easier because digital copies can be disseminated without loss of quality. Copyright management in a business context requires integrative conceptualization to protect innovation while maintaining the economic value of intellectual works (Mardikaningsih & Darmawan, 2023). Cross-border online trade adds complexity to law enforcement, as infringement claims must navigate dual jurisdictions and differing national rules. Handling these violations demands collaboration between rights holders, digital platforms, and law enforcement agencies to balance the protection of innovation with public access.

Finally, the emergence of algorithmic manipulation practices and the misuse of platforms to influence social and political processes represent more covert yet far-reaching forms of violations. Activities such as structured disinformation dissemination, the use of bots to manipulate public opinion, and the exploitation of recommendation mechanisms to

polarize audiences can undermine the integrity of democratic processes and public trust. Although they often appear as communication strategies, these practices can meet the elements of unlawful acts when they involve fraud, illicit financing, or violations of campaign regulations. The description of these types of violations is important before further discussion because it emphasizes that the digital medium requires a qualitative understanding of the character of actions and the adaptation of legal instruments that uphold basic principles without ignoring technical nuances.

The change in patterns of legal violations in the era of digital technology can be explained through a shift in the medium of action and how that action is understood as an act with juridical consequences (Grujić, 2018). The digital medium shortens the distance between intent and action because an act can be carried out through a few touches, then immediately produce consequences for other parties. At the same time, this medium expands the reach of action because information distribution and transactions can cross territorial boundaries. This shift causes violations that previously required physical encounters to now occur through the representation of accounts, messages, or electronic documents. Within a normative framework, this demands a reaffirmation of the relationship between the elements of the act, the element of fault, and accountability. Digital acts often appear as ordinary communication activities, yet they can fulfill the elements of unlawful conduct when fraud, deprivation of rights, system destruction, or attacks on honor are involved. Therefore, the discussion of violation patterns needs to understand that the digital medium changes the form of the action, not the fundamental legal principles. The principles of legality, fault, and evidence remain decisive, but their application requires a more precise understanding of the character of digital actions.

A crucial characteristic of the pattern of legal violations through digital technology lies in its layered nature. A single action can involve user devices, applications, network services, and platform providers, making the chain of acts complex (Harnowo, 2022). This complexity raises issues in determining the causal relationship between individual actions and the resulting harm, especially when the harm is influenced by the actions of multiple parties. Normatively, such complexity demands

a distinction between the perpetrator, the accomplice, and the party providing the facilities. This distinction cannot be resolved through moral intuition alone, but rather through an assessment of control, knowledge, and tangible contribution to the occurrence of the violation. In the digital space, contributions can take the form of designing fraud schemes, distributing tools, or setting up service architectures that facilitate misuse. However, service providers can also act as neutral intermediaries who do not have adequate knowledge of the unlawful acts committed by users. Thus, the changing pattern of violations drives a conceptual need to assess responsibility based on the degree of control and the reasonableness of prevention efforts, without blurring the limits of criminal liability that require fault.

Relative anonymity in the digital space also shapes the pattern of violations as it changes the perception of risk and the sense of being monitored (Acha, 2019). When someone feels their identity is protected, the psychological barriers to committing a violation can decrease. However, normatively, anonymity is not an excuse, but rather a situational factor that influences the choice of action. In many digital acts, identity can be disguised through fake accounts, temporary numbers, or service intermediaries, making it difficult for victims to identify the perpetrator. This difficulty can prolong the law enforcement process and increase the space for repeat violations. Within a legal framework, the main issue is not the existence of anonymity, but rather how to prove the link between a digital identity and a real legal subject. Therefore, patterns of violation in the digital era tend to emphasize the mastery of disguise skills, the management of footprints, and the utilization of procedural weaknesses. This demands an affirmation of the principle that actions carried out through a digital identity can still be assessed as legal acts, as long as the evidence is able to show a responsible relationship between the perpetrator and the act. At this point, the change in the pattern of violations is directly connected to the change in the pattern of evidence.

The patterns of legal violations in the digital space often rely on replication and redistribution. Information, images, and documents can be duplicated without loss of quality, then distributed to many people in a short time. From a normative perspective, this replication affects how the consequences of an act and the degree of fault are assessed (Russkevich et

al., 2022). A single post made without consideration can cause long-lasting reputational damage because the content circulates beyond the perpetrator's control. However, the fact that the perpetrator no longer controls the dissemination does not automatically erase the responsibility for the initial act, as responsibility is attached to the decision to make the content available to the public or a specific group. On the other hand, the act of redistribution by other parties raises questions about follow-up liability, especially if the redistribution is done with the intent to humiliate, extort, or incite. Thus, changing patterns of violations demand a tiered understanding of initial perpetrators and subsequent perpetrators. This understanding also needs to distinguish between redistribution that is informative in nature and redistribution that intensifies the harm. Consequently, the digital space changes the scale and duration of consequences, so normative assessments of the proportionality of sanctions and recovery need to consider the nature of replication and the perpetrator's ability to foresee the dissemination.

Digital technology changes the pattern of violations through a shift from physical violence toward symbolic and economic violence occurring through information (Agustina, 2015). Many violations no longer depend on direct coercion, but rather on the manipulation of perception, control of access, and exploitation of trust. Online fraud, extortion based on private content, and identity theft show that violations can operate through social engineering. Within a legal framework, social engineering challenges the way intentionality is assessed because the perpetrator uses a series of communications that appear reasonable to deceive the victim. However, that series can still be understood as an action directed toward obtaining gain by unlawful means. This pattern teaches that violations in the digital era often combine technical skills with the ability to read the emotions and habits of the victim. Therefore, the discussion of violation patterns needs to focus attention on the mechanisms of persuasion, the use of false authority, and the construction of scenarios. Normatively, this strengthens the need to assess an act based on intent, the sequence of actions, and the circumstances created by the perpetrator to subdue the victim's will. Digital technology in this regard acts as an amplifying medium, as it provides communication channels that are fast, personal, and appear official.

The change in patterns of legal violations is also visible in the shift of the attacked objects, from tangible items toward data and access (Kapinus, 2022). Personal data, credentials, and authentication tokens can become targets because data has economic value and opens the door to other services. Violations against data can occur through theft, illicit purchase, or tricking users into surrendering access. Normatively, attacks against data require an understanding of ownership, mastery, and the right of control. Although data is not always viewed as an object in the classical sense, the law can still protect the interests of the data subject through the categories of privacy rights, confidentiality, and protection against misuse. Data-based violation patterns show that loss can take the form of loss of control, not just loss of money. Loss of control means an identity can be used for actions that create obligations or harm for the victim. This changes how loss is assessed as a juridical consequence. Thus, the change in the pattern of violations demands an affirmation that violations can damage dignity and autonomy, so that legal protection is not limited to material loss. Accordingly, digital technology expands the spectrum of interests that must be protected by the law.

In the digital space, the boundary between expression and violation is frequently debated because communication has become easy and documented. Speech that attacks honor, incites hatred, or spreads false information can occur through brief formats that are often detached from responsibility (Russkevich et al., 2022). Normatively, the challenge lies in distinguishing legitimate criticism from attacks that damage the rights of others. The primary distinction lies in the substance, the objective, and the manner of delivery. When speech is directed toward degrading dignity or triggering hostility toward specific groups, the element of unlawfulness can be formed through an assessment of intent and reasonably foreseeable consequences. However, law enforcement must ensure that restrictions do not expand into silencing. This demands precision in formulating elements, assessing evidence, and weighing protected interests. Patterns of violation in the digital era show that an act can be judged as unlawful even if performed in a format that appears casual. Therefore, changing patterns of violation demand an improvement in the quality of normative reasoning that balances freedom of expression with the protection of

honor and public order. Such reasoning rests on the principles of proportionality and certainty.

The pattern of legal violations through digital technology is influenced by the attention economy. Platforms facilitate content that provokes responses, causing some users to be tempted to create material that violates norms for the sake of reach. Normatively, the attention economy motive can strengthen the assessment of fault when a violation is committed consciously for reputational or financial gain. However, the attention economy can also magnify the victim's losses because content spreads widely through recommendation mechanisms. Ethics and legality in the dissemination of information, particularly regarding the privacy of incident victims in digital media, become essential aspects to prevent exploitation for the sake of content reach (Muhammad et al., 2023). Within a legal framework, this raises questions about the limits of platform responsibility for dissemination amplified by the system. As a concept, platform responsibility can be interpreted through the duty of care and the obligation to respond reasonably to reports. However, such an assessment must distinguish between realistic control and the demand for total control. The changing pattern of violations cannot be separated from the reality that systems can prioritize content that triggers conflict, thereby giving a technical push to violations of honor and privacy. In normative discussion, this is important because it shows that the digital medium shapes social incentives. The law needs to interpret these incentives to formulate fair obligations, including standards for handling problematic content, without eliminating user freedom. Thus, the pattern of violation is formed by the intersection between individual choices and platform incentive structures.

The change in violation patterns is also evident in the increasing use of automation to commit unlawful acts. Automation can take the form of scripts, bots, or systems that perform repetitive actions such as password attempts, mass sending of fraudulent messages, or draining service resources. Within a normative framework, automation raises questions about the attribution of acts, as the actions are carried out by systems controlled or installed by humans. In principle, liability can still be directed toward the subject who initiates, controls, or intentionally allows the system to operate for unlawful purposes. However, evidence

requires attention to the relationship between control and knowledge. Automation also changes the scale, as a single perpetrator can attack many targets in a short time. This scale affects the assessment of the seriousness of the act as well as the need for victim protection. Additionally, automation can target parties with weak digital literacy, thereby strengthening the exploitative element. Digital popular culture also plays a role in shaping the values and behaviors of the younger generation who interact with these automated systems (Kurniawan & Khayru, 2021). In normative discussion, automation demonstrates that violations do not always take the form of a one-time act, but rather a designed process. Therefore, assessing digital violations needs to consider planning, the use of tools, and repetition patterns as indicators of the intensity of fault. Digital technology here expands the capacity of the perpetrator and changes the risk structure.

The pattern of legal violations in the digital space is also influenced by public dependence on online services for transactions and administration. This dependence creates opportunities for misuse through page forgery, payment fraud, and transaction redirection. Normatively, dependence changes the standards of prudence for both users and service providers. It is reasonable for users to trust services that appear official, while service providers have an obligation to build adequate security. Legal protection for consumers of online-based loan services becomes extremely crucial amidst increasing public dependence (Faridi et al., 2023). When a violation occurs, the assessment of responsibility needs to distinguish between actual user negligence and system negligence that creates risk. However, this distinction must not become a reason to weaken victim protection. Consumer legal compliance when facing cases of digital banking account takeovers becomes one of the benchmarks in assessing this distribution of responsibility (Fitrotinisak et al., 2023). Violation patterns in the digital transaction space often exploit similarities in appearance and official language, such that victims perform actions that appear voluntary but are actually directed by manipulation. Within a legal framework, this strengthens the understanding that consent obtained through deception has no justificatory value. Therefore, the changing pattern of violations shifts the focus from physical coercion to coercion through information. Normative discussion needs to place transaction

security as a public interest, as trust in services is a prerequisite for economic order. Thus, digital technology forms violation patterns that target trust as the primary object.

The change in violation patterns is also related to the shift in the private sphere due to data collection and monitoring practices. Privacy violations can occur when data is collected without valid consent, used beyond its purpose, or shared with third parties. Normatively, privacy is part of dignity and autonomy, making privacy violations a breach of fundamental rights. However, the digital space causes the boundaries of consent to often become blurred because consent is expressed through clicks and lengthy terms. In normative discussion, it is important to assess whether such consent fulfills the principles of awareness and freedom. If consent is merely formal but not understood, legal protection needs to emphasize transparency obligations and purpose limitations. Patterns of privacy violations also occur through doxing, the dissemination of personal data to intimidate, or the surveillance of partners and families. These acts show that technology can be used to control others through information. Within a legal framework, such violations demand a firm understanding of the prohibition of data misuse and protection for victims from threats. The change in violation patterns demands an affirmation that the private sphere must still be respected even though interactions take place through devices. The law needs to ensure that technology does not become a tool for the normalization of surveillance that degrades dignity.

The digital space also gives rise to violation patterns related to intellectual property rights, especially through the reproduction and distribution of works without permission. Normatively, these violations affect the interests of creators and the sustainability of the creative ecosystem. However, the digital medium makes reproduction cheap and fast, so some people view violations as commonplace. This normalization affects the formation of intent, as perpetrators may consider their actions reasonable. Nevertheless, ignorance or social habits do not automatically negate the unlawful nature of the act. The change in violation patterns in this area is related to the shift from physical piracy toward piracy through links, cloud storage, and content streaming. Obstacles in filing civil lawsuits by copyright holders often become a barrier to enforcing these

intellectual protection norms (Hardyansah et al., 2021). Therefore, normative discussion needs to assess how the elements of the act are manifested in the actions of uploading, sharing, or providing access. In the digital space, the act of providing access can be equivalent to distribution, as access facilitates the public in obtaining the work. However, enforcement also needs to distinguish between scale and purpose, for example, for commercial gain or for limited use. This distinction is important to maintain proportionality. Thus, digital technology changes the way violations are committed, while the principle of protecting rights remains the basis of assessment.

The change in legal violation patterns is also visible in the increasing conflict regarding reputation through social platforms. Defamation, bullying, and coordinated attacks can occur through groups of accounts that amplify certain narratives. Normatively, reputation is a protected interest because it is linked to a person's honor and social opportunities. The digital medium expands the space for public judgment, so reputation can be damaged through repetitive narratives. This repetition is often more damaging than a single statement, as it creates an impression of truth through intensity. In normative discussion, it is important to assess the elements of the act and fault in actions that orchestrate attacks, including the use of fake accounts and incitement. The assessment also needs to consider the victim's position, as victims can experience an inability to defend themselves when narratives spread rapidly. However, reputation protection must be structured in harmony with freedom of expression. The application of restorative justice in resolving speech cases in the digital space can be a balanced alternative solution from a legal perspective (Darmawan & Negara, 2023). Therefore, the change in violation patterns in the realm of reputation demands precision in assessing the difference between fact-based criticism, opinions, and harmful false accusations. The evidentiary process will depend heavily on digital footprints, dissemination chains, and account interconnections. Thus, digital technology makes reputation an easy target for attack, necessitating legal norms to provide firm boundaries against actions that unlawfully damage honor.

Another characteristic of the digital violation pattern is the ease of forming communities that facilitate unlawful acts. These communities can take the form of forums, messaging groups, or sharing spaces that provide

technical knowledge and transaction opportunities. Normatively, the existence of such communities challenges the determination of boundaries between communication and conspiracy. When communication contains coordination to perform an unlawful act, the element of fault can be formed through shared intent and the division of tasks. However, proof requires attention to the content of communication and subsequent actions. In the digital space, communication can be disguised through codes, specific terms, and the fragmentation of information across multiple messages. This demands careful law enforcement to avoid haphazardly concluding a conspiracy. Social media mediates the development of digital literacy among youth, which must be balanced with legal awareness to prevent collective deviance (Kurniawan, Darmawan, & Khayru, 2021). On the other hand, normative assessments need to pay attention to parties providing the means of meeting if those means are consciously used to facilitate violations. However, such obligations must be limited so as not to turn into excessive control over legitimate conversations. Thus, the change in violation patterns shows that the solidarity of perpetrators can be built through intense digital interaction. This pattern shifts the dynamics of violations from individual actions toward collective actions, allowing liability to expand according to each party's role within the network.

Digital technology shapes violation patterns through the ability to create synthetic material that resembles reality. Synthetic material can be used to deceive, extort, or damage reputations. Normatively, synthetic material challenges the concept of factual truth in evidence, as visual evidence that was once considered strong can now be questioned. Within a legal framework, this issue does not mean that electronic evidence becomes weak, but rather demands stricter verification procedures. Furthermore, the use of synthetic material to manipulate victims demonstrates a clear intent, as the perpetrator constructs tools to create false beliefs. Thus, changes in violation patterns in this area strengthen the element of planning as an indicator of fault. On the victim's side, synthetic material can cause psychological pressure and social harm, as the public tends to react quickly before verification occurs. The juridical analysis of the validity of electronic contracts involving intelligent systems becomes crucial in determining the validity of legal acts in the digital era (Maulani

et al., 2023). In normative discussion, it is important to emphasize that the creation and distribution of synthetic material for the purpose of deceiving or extorting are infringing acts, regardless of the technological sophistication. At the same time, the law needs to distinguish the legitimate use of synthetic material in creative works from its use for fraud. This distinction requires an assessment of purpose, distribution method, and reasonably foreseeable consequences. Digital technology here changes the form of the tool, while the norm evaluates the orientation of the act.

The pattern of legal violations in the digital space is also influenced by cross-border jurisdictions. Perpetrators can be in a different territory from the victims, servers, and service providers. Normatively, these cross-border elements raise questions about authority, cooperation, and the application of national norms to actions occurring through a global network. However, cross-border nature does not negate the unlawful character of an act against a real victim. The main challenge is the enforcement mechanism, not the definition of fault. In normative discussion, it must be understood that legal certainty demands coordination between authorities and procedures that respect both the rights of the suspect and the rights of the victim. The cross-border nature also affects evidence collection, as electronic evidence may reside with foreign service providers. This demands valid request procedures and the maintenance of evidence integrity. Risk mitigation on cross-regional digital platforms is a concrete form of legal protection for the parties involved (Sahid et al., 2023). Violation patterns may exploit cooperation gaps by moving services or splitting transactions across several regions. Therefore, changing violation patterns drive the need to strengthen the principles of due process in cooperation. These principles ensure that enforcement does not sacrifice the protection of rights. Thus, digital technology demands the structuring of relationships between jurisdictions as part of the normative response to cross-border violations.

Digital technology also shapes violation patterns through a shift in time, as actions can occur asynchronously. Perpetrators can commit an act at any time, victims may realize the loss later, and evidence may appear after certain traces are collected. Normatively, asynchronicity affects assessments of immediacy, reporting, and recovery. For example, the dissemination of content that damages honor can continue to cause harm

even if the initial upload occurred long ago. This demands an understanding of the continuity of consequences and responsibility for ongoing distribution. However, such understanding must maintain reasonable limits to avoid creating uncertainty. In the realm of digital transactions, asynchronicity can cause victims to lose the opportunity to prevent losses because warnings arrive too late. Recognition of the validity of electronic instruments becomes a decisive aspect in providing legal certainty for every asynchronous digital activity (Sulaiman et al., 2023). In normative discussion, this reinforces the importance of reporting obligations and rapid responses from service providers. Asynchronicity also changes the pattern of violations into a sequence; for instance, a perpetrator might test a victim with small messages before escalating to a larger fraud. Therefore, the law needs to read patterns as a series of actions rather than isolated fragments. Reading the sequence helps in assessing intent and planning, making accountability more accurate. Thus, the change in violation patterns in the digital era is closely linked to the flexible nature of time within networks.

In law enforcement, the change in digital violation patterns is closely linked to electronic evidence. Evidence can take the form of access logs, transaction histories, metadata, screenshots, and communication recordings. Normatively, evidentiary procedures require principles of integrity, relevance, and lawful acquisition. Without integrity, evidence is easily disputed because it can be altered or fabricated. Without relevance, evidence becomes a heap of information that fails to explain the act. Without lawful acquisition, enforcement risks violating rights and damaging the legitimacy of the process. Changing violation patterns make the evidentiary process increasingly dependent on the ability to verify origin, chain of custody, and the link between accounts and legal subjects. Professional integrity within the legal system is crucial to maintaining justice and material truth in this evidentiary process (Saktiawan et al., 2021). In normative discussion, it is important to emphasize that electronic evidence must not be simplified into reliance on a single screenshot. Assessments must weigh the possibility of forgery, manipulation, or extra-procedural acquisition. On the other hand, this caution must not turn into excessive skepticism that hinders victim protection. Therefore, the law needs to place electronic evidence within a

systematic reasoning framework. Digital technology changes the form of evidence, while evidentiary norms provide the standard to evaluate its truth fairly.

The pattern of legal violations through digital technology also raises issues concerning negligence. Many incidents occur due to weak security, ignored updates, or irresponsible password sharing. Normatively, negligence can serve as a basis for liability within certain limits, especially when there is a clear duty of care. However, a distinction must be made between the negligence of individual users and the negligence of organizations managing systems. Organizations often possess greater capacity and obligations to protect data and services. Thus, the change in violation patterns demands attention to standards of reasonable security. These standards should not be purely technical but must relate to governance, training, and response procedures. In normative discussion, it is vital to assess whether negligence opened the door for the perpetrator and whether the loss was a reasonably foreseeable consequence. Responsive law enforcement is necessary to address various forms of malpractice and violations in professional services involving negligence (Safitri et al., 2023). However, the victim's negligence must not be used as an excuse to pardon a perpetrator who commits an unlawful act intentionally. This distinction maintains justice, as the primary perpetrator remains responsible for their intent and actions. Accordingly, digital technology changes the risk landscape, requiring the concept of negligence to be understood as part of security governance and reasonable behavior in system usage.

Digital technology also drives changes in the pattern of violations within the realm of consumer protection. Digital products and services often offer convenience, yet they can conceal terms, costs, or data usage practices. Normatively, violations can occur when business actors engage in misleading information, coerce consent through manipulative designs, or complicate the termination of services. These manipulative practices demonstrate that legal violations do not always take the form of classic criminal acts, but can instead manifest as violations of consumer protection principles and contractual fairness. The legal validity of these modern transactions is increasingly relevant, as seen in the juridical analysis of the validity of electronic contracts made by artificial intelligence

in Indonesian law (Maulani et al., 2023). In normative discussion, it is important to assess whether user consent arises from adequate understanding. When consent is obtained through intentionally created confusion, it loses its legitimate value. Violation patterns in this area often rely on information asymmetry, where business actors understand the system while users are in a weak position. Therefore, the law needs to evaluate standards of transparency, honesty, and design fairness. The change in violation patterns is also visible in the use of unilateral agreement updates that alter user rights. Normatively, unilateral changes demand an examination of the principle of good faith. Digital technology in this regard provides tools to modify legal relationships rapidly, so norms must provide boundaries that keep the user's position protected.

Digital violation patterns can involve children and adolescents as both victims and perpetrators, as device access becomes easier and family supervision varies. Normatively, the protection of children demands special attention to the risks of exploitation, image-based extortion, and bullying. However, when a child becomes a perpetrator of an infringing act, legal assessment needs to consider psychological development and the objectives of guidance. This shift is influenced by how social media and contemporary youth digital literature shape modern social interactions (Kurniawan, Darmawan, & Khayru, 2021). The change in violation patterns in this area occurs because private communication can be conducted through platforms that appear safe. Adult perpetrators can infiltrate through false identities, build trust, and then exploit closeness for unlawful purposes. In normative discussion, it is vital to affirm the protection obligations of platforms and service providers, especially regarding reporting and the termination of access for problematic accounts. However, such obligations must be structured with mechanisms that maintain accuracy to avoid false accusations. Child protection also demands legal literacy and digital ethics in education, as social prevention is linked to the formation of awareness regarding boundaries. Thus, digital technology changes the pathways of encounters between perpetrators and victims, requiring child protection norms to emphasize safety, dignity, and recovery while still upholding the principles of justice.

Digital technology changes the pattern of violations through the ease of gathering masses and directing collective action. Coordinated attacks,

mass reporting intended to shut down accounts, or chain dissemination of slander can occur through a brief call to action. Normatively, such collective actions demand a distinction between voluntary participation and participation triggered by incitement. When a party directs a mass to harm others, the element of fault can be formed through the intent to mobilize and the knowledge that harm might occur. Legal protection in these digital interactions is essential, including for participants in activities like online arisan engagements (Negara & Darmawan, 2023). However, proof requires a link between the mobilizer and the executors, including communication trails. The change in violation patterns in this area shows that harm can occur through the accumulation of small actions, such as abusive comments made by many people. In normative assessment, accumulation challenges the concept of a single perpetrator, such that liability can be dispersed. However, the dispersion of responsibility does not mean responsibility disappears. The law needs to assess the contribution of each party based on role and intent. Additionally, platforms have a procedural obligation to manage reporting so that it is not used as a tool for oppression. Thus, digital technology forms violation patterns that rely on mass dynamics, necessitating that norms maintain a space for healthy public participation while rejecting collective actions that undermine the rights of others.

Digital violation patterns are also related to system intrusion and unauthorized access. These acts can take the form of hacking, installation of malicious software, or account takeovers. Normatively, unauthorized access violates the principle of user sovereignty over their system and breaches public security. However, these acts are often debated when performed under the pretext of security testing or research. Normative discussion needs to distinguish authorized research with protective goals from actions that exploit vulnerabilities for personal gain or damage. Maintaining justice in such complex adversarial systems requires high professional integrity and ethical principles in legal advocacy (Saktiawan et al., 2021). This distinction rests on consent, scope, and good faith. If access is performed without permission, the element of unlawfulness tends to be fulfilled, even if the perpetrator claims they had no intent to cause damage. In the digital space, unauthorized access can lead to further harm, as the perpetrator can steal data, alter systems, or open doors for other actors.

Therefore, the change in violation patterns in this area reinforces the importance of security as a collective interest. Normative assessment needs to treat the mastery of technical tools as an aggravating factor when used unlawfully. However, enforcement also needs to provide room for responsible vulnerability reporting through legal mechanisms. Thus, digital technology expands the possibilities of access, so norms must affirm the boundaries of permission and the duty of care.

Digital technology shapes violation patterns through black markets that trade in data, access, and illegal services. These markets connect perpetrators with buyers, provide false reputations, and create an ecosystem of incentives. Normatively, the trade of tools and data for unlawful acts gives rise to independent liability, as such actions facilitate further violations. However, evidence requires an assessment of the seller's knowledge regarding the intended use. When a seller knows that goods or data are being used for a violation, the element of fault can be established. This ecosystem often involves complex financial interactions, necessitating a legal perspective on investment risk mitigation, particularly on peer-to-peer lending platforms (Sahid et al., 2023). Violation patterns in this area also change the relationship between perpetrator and victim, as the primary perpetrator can purchase access without ever knowing the victim. This renders violations more industrialized. In normative discussion, this phenomenon demands an evaluation of the violation supply chain, from data thieves and intermediaries to the perpetrators executing the fraud. Law enforcement that only targets the end-perpetrator risks allowing the ecosystem to survive. However, the normative approach must maintain the certainty of the elements of the offense and avoid the groundless expansion of liability. Thus, digital technology encourages the formation of markets that reinforce violations, necessitating that norms interpret the trade of illegal facilities as part of the changing pattern of violations.

The change in digital violation patterns also transforms the relationship between the victim and recovery. Many victims face difficulties in restoring reputation and privacy because content can reappear through re-uploads. Normatively, recovery requires effective mechanisms for deletion, correction, and dissemination restrictions, while still respecting the rights of other parties. However, recovery does not always mean total deletion, as there are specific public interests that must

be maintained. Ethics and legality are paramount when disseminating information through digital media, especially regarding traffic accident victims (Muhammad et al., 2023). The distinction between public interest and voyeuristic interest becomes crucial. In normative discussion, recovery is also related to protection from revictimization. When the reporting process requires the victim to repeat their trauma through the presentation of evidence, procedures must uphold the victim's dignity. Additionally, economic recovery for victims of digital fraud demands rapid mechanisms because losses can spread through numerous accounts and intermediaries. Although this writing does not present technical procedures, it can be normatively affirmed that recovery requires institutional coordination and victim service standards. Thus, changes in violation patterns necessitate an understanding of recovery as part of substantive justice, rather than merely the imposition of sanctions. Digital technology expands the scope of harm; therefore, recovery norms must adjust the form of protection.

Digital violation patterns also demand a re-reading of the public and private spheres within communication spaces. Closed group conversations can be leaked, disseminated, and used to harm others. Normatively, the dissemination of private conversations without consent can violate privacy rights, especially when the content involves sensitive data. The study by Muhammad et al. (2023) reinforces that ethics and legality in information dissemination on digital media serve as the primary foundation for preventing harm to subjects whose data is exposed. However, there are certain circumstances where disclosure may be justified for the purpose of reporting a violation. Therefore, normative discussion needs to assess the reasons for disclosure, proportionality, and objective. Violation patterns emerge when individuals exploit digital intimacy to obtain material that can be used as a tool for extortion. These acts show that violations can originate from relationships that appear voluntary. Thus, norms need to affirm that consent at one stage does not imply consent for dissemination at another stage. Evidence also becomes complicated because the perpetrator and victim share a long communication history. In normative discussion, the assessment must separate the element of the personal relationship from the element of the unlawful act. Accordingly, digital technology changes the boundaries of conversation, so the law must protect the dignity and freedom of communication without allowing

harmful misuse. The core principle remains the protection of rights and the fair assessment of intent.

The change in violation patterns through digital technology creates a need to reassess the proportionality of sanctions. In the digital space, harm can spread rapidly, yet perpetrators can vary from organized actors to users acting impulsively. Normatively, proportionality demands sanctions that are commensurate with the fault, the harm caused, and the circumstances of the perpetrator. Sanctions that are too severe risk exceeding the purposes of punishment, while sanctions that are too light risk ignoring victim protection. Therefore, normative discussion needs to emphasize the distinction between planned actions and those occurring due to serious negligence. This distinction is not intended to justify violations, but rather to maintain justice. This approach is relevant to the thoughts of Negara and Darmawan (2023), who emphasize the importance of legal protection and certainty in digital interactions to ensure user safety. Furthermore, sanctions in the digital space need to consider recovery aspects, such as the obligation to delete content, valid apologies, or the restoration of losses, insofar as recognized by law. However, recovery must not be used as a tool for pressuring the victim. Thus, digital technology expands the spectrum of violations, so the assessment of sanctions requires subtle and rigorous normative reasoning, oriented toward the protection of rights and legal certainty.

Digital violation patterns also raise questions about legal education and ethics as part of prevention. Many infringing acts occur due to habit, group influence, or a lack of understanding regarding legal boundaries. Normatively, prevention requires the formation of awareness that the digital space is a legal space. Contemporary digital literacy education for the younger generation is a key to prevention, as outlined by Kurniawan, Darmawan, and Khayru (2021) regarding behavioral dynamics on social media. This awareness includes an understanding of privacy, honor, copyright, and the prohibition of fraud. Education cannot be understood as a substitute for enforcement, but rather as a complement that builds voluntary compliance. In normative discussion, education also needs to touch upon the responsibilities of platforms and organizations, as users interact within environments shaped by design. Clear and transparent design can encourage compliance, whereas manipulative design can

encourage deviance. Therefore, the change in violation patterns shows that prevention relates to both social norms and legal norms simultaneously. When social norms downplay digital violations, law enforcement becomes difficult because social legitimacy is weak. Thus, normative discussion demands attention to the formation of public norms that respect dignity and rights. Digital technology accelerates the spread of behavior, so education and the affirmation of norms must go hand in hand to resist the normalization of violations.

Digital technology shapes changes in the pattern of legal violations through three main pathways: the shift in the form of acts, the shift in accountability relations, and the shift in evidence. The shift in the form of acts is evident in the transition from physical actions toward actions based on information, data, access, and repetitive communication. The shift in accountability relations is visible in the involvement of multiple actors and intermediaries, such that the assessment of fault must interpret control, knowledge, and contribution to the occurrence of the violation. The shift in evidence is seen in the dominance of electronic traces that demand integrity, verification, and lawful acquisition procedures. This is in line with the analysis of Maulani et al. (2023) regarding the validity of electronic contracts and digital footprints which require legal certainty in modern judicial systems. These three pathways are interconnected. When the form of an act changes, the relationship between perpetrator and victim changes, and subsequently, the need for evidence also changes. Normative discussion shows that fundamental legal principles remain the basis, yet their application requires a more precise interpretation of the character of the digital medium. Thus, the change in violation patterns is not merely an addition of types of acts, but a change in the structure of action and assessment. This framework helps in understanding how the law can continue to guarantee certainty and justice when the social medium changes. The affirmation of boundaries, the precision of evidence, and the differentiation of roles constitute the core of the conceptual explanation regarding the change in patterns of legal violations in the digital era.

Conclusion

Digital technology shapes changes in the patterns of legal violations by transforming how actions are committed, how responsibility is linked, and how the truth of an event is proven. The digital medium expands the reach of actions, accelerates dissemination, and enables acts based on identity representation, data, and access. These changes give birth to patterns of violation that emphasize information manipulation, identity misuse, attacks on data, and recurring reputational damage through content distribution. Normatively, this shift demands a more precise interpretation of the elements of action and fault (*mens rea*), especially when actions occur through service chains and involve multiple parties. At the same time, electronic evidence becomes a key point because digital trails serve as the primary tool for connecting accounts, events, and legal subjects. Within this framework, the discussion answers the problem formulation by demonstrating that changes in violation patterns represent a shift in the structure of action and assessment, while the principles of legality, justice, and certainty remain the primary references in law enforcement.

The implications and suggestions that can be drawn are the need to strengthen the normative framework that asserts the limits of responsibility based on control, knowledge, and contribution, ensuring that assessments do not fall into the trap of oversimplification between individuals and platforms. Law enforcement needs to place electronic evidence within procedures that maintain the integrity of the evidence and respect rights, so that the legitimacy of the process is preserved. At the policy level, clearer guidelines are needed regarding the duty of care for service providers, particularly in data security, report handling, and procedural transparency, without encouraging excessive surveillance. At the community level, digital legal literacy needs to be directed toward the understanding that communication, transactions, and data management have juridical consequences. In the educational sphere, the formation of digital ethics must strengthen respect for the dignity, privacy, and honor of others. Academically, further conceptual development can enrich the distinction between information-based violations and access-based violations, as well as formulate the principle of proportionality that is sensitive to the scale of dissemination and the planning of actions in digital space.

References

Acha, F. R. 2019. Crimes Digitais: Uma Necessária Releitura Do Direito Penal À Luz Das Novas Tecnologias. *Linkscienceplace - Interdisciplinary Scientific Journal*, 5(6), 13-99.

Agustina, J. R. 2015. Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology*, 9(1), 35–54.

Anugroh, Y. G., Hardyansah, R., Darmawan, D., Khayru, R. K., & Putra, A. R. 2023. Consumer Protection and Responsibilities of E-commerce Platforms in Ensuring the Smooth Process of Returning Goods in COD Transactions. *Journal of Social Science Studies*, *3*(2), 89-94.

Aziz, A., Darmawan, D., Khayru, R. K., & Wibowo, A. S. 2023. Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. *Journal of Social Science Studies*, *3*(1), 23-28.

Bailey, K. 2008. *Methods of Social Research*. Simon and Schuster, New York.

Darmawan, D. 2021. Social Interaction in Digital Society: Changes in Online Communication Patterns and Dynamics of Virtual Communities, *Studi Ilmu Sosial Indonesia,* 1(1), 325-350.

Darmawan, D. 2023. Developing Pedagogical Standards and AI Policies for Adaptive Learning in Equitable and Safe School Education. *Journal of Practice Learning and Educational Development*, *3*(4), 400-413.

Darmawan, D., & Negara, D. S. 2023. The Application of Restorative Justice in Resolving Speech Cases in the Digital Space: A Normative Analysis of the Electronic Information and Transactions Law and the Criminal Code. *Journal of Social Science Studies*, *3*(1), 295-306.

Diantha, I. M. P. 2016. *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*. Prenada Media, Jakarta.

Faridi, F., Darmawan, D., Hardyansah, R., Putra, A. R., & Wibowo, A. S. 2023. Legal Protection for Online-Based Lending Consumers. *International Journal of Service Science, Management, Engineering, and Technology*, *4*(2), 34-38.

Fitrotinisak, I. K., Mardikaningsih, R., Gautama, E. C., & Vitrianingsih, Y. 2023. Legal Compliance for Consumers in Dealing with Cases of Account Tampering in Digital Banking Services. *Journal of Social Science Studies*, *3*(1), 75-82.

Grujić, Z. 2018. Cybercrime: Specificity and Contemporary Challenges. *Zbornik Radova Pravnog Fakulteta u Nišu*, 57(80), 325–346.

Hamid, S. 2023. Rationalization of Technological Criminology in the Era of Disruption. *International Journal on Social Sceince, Economics and Art*, 12(4), 221–232.

Handoko, C. 2017. Kedudukan Alat Bukti Digital dalam Pembuktian Cybercrime di Pengadilan. *Jurisprudence,* 6(1), 1–15.

Hardyansah, R., D. Darmawan, & D. S. Negara. 2021. Analysis of Inhibiting Factors in the Filing of Civil Lawsuits by Copyright Holders, *Studi Ilmu Sosial Indonesia*, 1(2), 223-248.

Harnowo, T. 2022. Law as Technological Control of the Infringement of Intellectual Property Rights in the Digital Era. *Corporate and Trade Law Review*, 2(1), 65–79.

Henn, M., M. Weinstein., & N. Foard. 2005. *A Short Introduction to Social Research*. Sage, London.

Ivanov, A., D. Gorelik., & K. Prokofiev. 2021. Law Enforcement in the Context of Digitalization: Problems and Prospects for Improving Efficiency. In *1st International Scientific Conference" Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development"(LARDER 2020)*, 125–130.

Kapinus, O. 2022. Digitalization of Crime and Criminal Law. *Baikal Research Journal*, 13(1), 22-28.

Kolesov, M. V. 2021. On the Impact of Digital Technologies on Modern Society. *Russian Journal of Legal Studies (Moscow)*, 8(2), 23–27.

Kurniawan, Y. & R. K. Khayru. 2021. Popular Culture and Youth: Value, Attitude, and Behavior Formation Through Music, Film, and Digital Content, *Studi Ilmu Sosial Indonesia*, 1(1), 303-324.

Kurniawan, Y., D. Darmawan, & R. K. Khayru. 2021. Social Media and Contemporary Youth Digital Literature, *Studi Ilmu Sosial Indonesia*, 1(2), 109-124.

Loeckx, J. 2016. Blurring Boundaries in Education: Context and Impact of MOOCs. *International Review of Research in Open and Distributed Learning*, 17(3), 92-121.

Mardikaningsih, R., & Darmawan, D. 2023. An Integrative Conceptualization for Copyright Management in a Business Context. *Legalis et Socialis Studiis (L355)*, *1*(2), 14-24.

Maulani, A., Hardyansah, R., Darmawan, D., Mendonca, C. N., & de Jesus Isaac, A. 2023. Juridical Analysis of the Validity of Electronic Contracts Made by Artificial Intelligence in Indonesian Law. *Journal of Social Science Studies*, *3*(1), 139-144.

Muhammad, A. I., Saputra, R., Pakpahan, N. H., Darmawan, D., & Khayru, R. K. 2023. Ethics and Legality in the Dissemination of Information on Traffic Accident Victims Through Digital Media. *Journal of Social Science Studies*, *3*(2), 235-244.

Negara, D. S., & Darmawan, D. 2023. Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, *2*(2), 13-19.

Oriento, C., Negara, D. S., Putra, A. R., Arifin, S., & Saputra, R. 2023. Risks and Legal Protection in Non-Cash Financial Transactions Through E-Wallets. *Journal of Social Science Studies*, *3*(1), 109-114.

Putra, A. R., Darmawan, D., & Arifin, S. 2023. Digital Sharia Finance Products and Service Innovation Under Managerial Governance. *Studi Ilmu Sosial Indonesia*, 3(1), 129-158.

Rakhmanova, E. N., & T. V. Pinkevich. 2020. Digital Crime Concept. In *2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth"(MTDE 2020)*, 193-196.

Russkevich, E., A. P. Dmitrenko., & N. G. Kadnikov. 2022. Crisis and Palingenesis (Rebirth) of Criminal Law in the Context of Digitalization. *Vestnik Sankt-Peterburgskogo Universiteta*, 13(3), 585–598.

Safitri, N., Gautama, E. C., Issalillah, F., Mardikaningsih, R., & Vitrianingsih, Y. 2023. Law Enforcement Against Midwife Malpractice in Midwifery Services in Indonesia. *Journal of Social Science Studies*, *3*(2), 1-10

Sahid, R. R., Hardyansah, R., Darmawan, D., Negara, D. S., & Khayru, R. K. 2023. Legal Perspective of Investment Risk Mitigation on Peer-to-peer Lending Platforms. *Journal of Social Science Studies*, *3*(1), 177-184.

Saktiawan, P., Hardyansah, R., Darmawan, D., & Putra, A. R. 2021. Ethical Principles in Indonesian Legal Advocacy: Sustaining Justice in Adversarial Systems Through Professional Integrity. *Journal of Social Science Studies*, *1*(2), 239-244.

Sasmita, B., Darmawan, D., & Khayru, R. K. 2023. Telemedicine regulation in Indonesia: Enhancing patient safety and protection. *International Journal of Service Science, Management, Engineering, and Technology*, *4*(3), 29-35.

Sinambela, E. A. 2022. The Digital Public Sphere Under Threat of Disinformation a Literature Study on Hoax Dissemination Dynamic and Vulnerability Factors, *Studi Ilmu Sosial Indonesia*, 2(2), 289-306.

Sulaiman, M., Pakpahan, N. H., & Putra, A. R. 2023. Analysis of the Validity and Effectiveness of Electronic Contracts in Legal Protection of Digital Transactions in Indonesia. *Journal of Social Science Studies*, *3*(1), 41-46.

Wibowo, A. S., Darmawan, D., Halizah, S. N., & Mardikaningsih, R. 2023. Optimizing the Principles of Healthy Business Competition and the Role of KPPU for a Fair Economy in the Digital Era. *Journal of Social Science Studies*, *3*(1), 95-100.

Wibowo, A. S., Darmawan, D., Negara, D. S., & Hardyansah, R. 2023. Analysis of Value Added Tax Application on Electronic Commerce Transaction in Digital Economy System in Indonesia. *Journal of Social Science Studies*, *3*(2), 83-88.

Zimdars, M., & K. McLeod. (Eds.). 2020. *Fake News: Understanding Media and Misinformation in the Digital Age*. MIT Press, Cambridge.