

# ANAYASA

(Journal of Legal Studies)

E-ISSN: 2987-9965

Vol.4, No. 1, Juli 2026

## PERSONAL DATA PROTECTION AND LAW ENFORCEMENT AGAINST INFORMATION MANIPULATION ON SOCIAL MEDIA

<sup>\*1</sup>Rochmadi Wicaksono, <sup>2</sup>Edi Saputra Hasibuan

<sup>\*1,2</sup>Universitas Bhayangkara Jakarta Raya

Email: <sup>\*1,2</sup>rochmadiwicaksono@gmail.com

### Abstract

Advances in information and communication technology have brought about significant changes in the use of social media as a means of communication and information exchange in society. However, these advances have also given rise to new legal issues, particularly regarding the protection of personal data and the manipulation of digital information. This study aims to analyze the forms of legal protection for the personal data of social media users based on Indonesian laws and regulations, as well as to examine the effectiveness of law enforcement against information manipulation from a cyberlaw perspective. The research method used is normative legal research employing both a statutory and a conceptual approach. The results show that legal protection for personal data is regulated by the Electronic Information and Transactions Law and the Personal Data Protection Law, which recognize the right to privacy, the obligations of data controllers, and administrative and criminal sanctions for personal data violations. However, implementation still faces various obstacles, such as low levels of digital literacy among the public and limited oversight. Meanwhile, law enforcement against information manipulation on social media has not been effective due to limitations in legal substance, the capabilities of law enforcement officials, and technological challenges such as deepfakes and the borderless nature of the internet. Therefore, it is necessary to strengthen regulations, enhance the capacity of law enforcement officials, and improve the public's digital literacy to create more effective legal protection in the digital age.

**Keywords:** Legal protection, personal data, social media, information manipulation

### Abstrak

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam penggunaan media sosial sebagai sarana komunikasi dan pertukaran informasi di masyarakat. Namun, kemajuan tersebut juga menimbulkan permasalahan hukum baru, khususnya terkait perlindungan data pribadi dan manipulasi informasi digital. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap data pribadi pengguna media sosial berdasarkan peraturan perundang-undangan di Indonesia serta mengkaji efektivitas penegakan hukum terhadap manipulasi informasi dalam perspektif hukum siber. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap data pribadi telah diatur melalui Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi, yang memberikan pengakuan terhadap hak privasi,

*kewajiban pengendali data, serta sanksi administratif dan pidana terhadap pelanggaran data pribadi. Namun, implementasinya masih menghadapi berbagai kendala, seperti rendahnya literasi digital masyarakat dan keterbatasan pengawasan. Sementara itu, penegakan hukum terhadap manipulasi informasi di media sosial belum berjalan efektif akibat keterbatasan substansi hukum, kemampuan aparat penegak hukum, serta tantangan teknologi seperti deepfake dan sifat internet yang borderless. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas aparat penegak hukum, serta peningkatan literasi digital masyarakat guna menciptakan perlindungan hukum yang lebih efektif di era digital.*

**Kata kunci:** *Perlindungan hukum, data pribadi, media sosial, manipulasi informasi*

## **INTRODUCTION**

The development of information and communication technology has brought fundamental changes to the patterns of modern society. Digital transformation has not only changed the way individuals communicate, acquire information, and build social relationships, but has also influenced various aspects of economic, political, educational, governmental, and law enforcement life. The presence of the internet and social media has created a digital public space that allows society to interact rapidly without being limited by space and time. Social media platforms such as Facebook, Instagram, X, TikTok, and various other digital communication applications have become an integral part of daily life. Society can independently produce, access, store, and distribute information at a speed previously not possible with conventional media. These changes provide great benefits in expanding access to information and increasing public participation, but at the same time also give rise to complex new legal issues, particularly related to personal data protection, information security, privacy, and digital information manipulation.

Within the digital ecosystem, personal data has developed into one of the assets with very high economic, social, and strategic value. Data concerning a person's identity, phone number, email address, location, preferences, online activity, transaction history, and even biometric information can be collected and processed for various purposes. Technology companies use user data to provide more personalized services, analyze consumer behavior, and develop data-driven marketing strategies. On the other hand, personal data can also be misused by certain parties for commercial, political, or cybercriminal purposes. The development of the digital economy has thus positioned personal data as a commodity with strategic value, while simultaneously creating new vulnerabilities to individual privacy rights (Solove, 2006).

The issue of personal data protection becomes increasingly complex when such data is processed through social media platforms. Social media users, consciously or unconsciously, leave large amounts of digital traces through uploads, comments, interactions, location data, preferences, and search activity. This data can be used to build a digital profile of a person and predict certain behaviors, preferences, or tendencies. In this context, privacy is no longer solely about the confidentiality of personal information, but also concerns an individual's right to control how information about themselves is collected, used, stored, and disseminated. Nissenbaum (2010) explains that privacy protection in the digital era cannot be adequately understood merely as an effort to

conceal information, but must also consider the appropriateness of information flow within a particular social context. Thus, the use of personal data without consent or outside its proper context can constitute a violation of an individual's privacy rights.

The misuse of personal data through social media can take various forms, ranging from identity theft, account takeover, unauthorized disclosure of personal data, use of information for fraud, to the exploitation of data to influence political preferences and public behavior. Illegally obtained data can also be used to create fake digital identities or conduct social engineering. In practice, perpetrators can exploit information available on social media to gain a victim's trust, then use that information to commit fraud, extortion, or other criminal acts. This condition shows that personal data protection is closely related to cybersecurity and the protection of society from various forms of digital crime (Bennett & Raab, 2006).

Alongside the issue of personal data misuse, the development of social media also presents a serious challenge in the form of information manipulation. Social media allows information to be produced and disseminated by anyone without going through the verification mechanisms found in conventional mass media. The speed of digital information dissemination is often not matched by users' ability to verify the truth of that information. As a result, false information, disinformation, misinformation, digital propaganda, and manipulative content can spread rapidly and reach a wide audience. Wardle and Derakhshan (2017) distinguish misinformation as false information that is not always shared with an intent to cause harm, while disinformation refers to false information that is deliberately created and disseminated to cause harm. In the context of cyber law, this distinction is important because the element of intent can determine the character and legal consequences of an act.

Information manipulation on social media can be carried out through various methods, such as the spread of fake news or hoaxes, image and video manipulation, digital identity engineering, the use of fake accounts, the exploitation of automated bots, and the exploitation of users' personal data to shape public opinion. The development of generative artificial intelligence also has the potential to increase the complexity of this issue through its ability to produce synthetic text, images, audio, and video that are increasingly difficult to distinguish from authentic content. The phenomenon of deepfakes, for example, can be used to manipulate a person's identity or create false narratives that have the potential to damage reputations and cause harm. Therefore, legal challenges in the digital space relate not only to false content, but also to the process of production, distribution, and use of the data underlying the creation of manipulative information.

Information manipulation accompanied by personal data misuse has a more complex legal dimension because it can involve several legal interests simultaneously. On one hand, there is an interest in protecting privacy rights and personal data security. On the other hand, there is an interest in maintaining the integrity of digital information and protecting society from harmful content. If false information is disseminated using a victim's personal data, such an act can cause layered harm, whether to the victim's privacy, dignity,

security, or economic interests. In certain conditions, personal data misuse can also become part of a broader chain of cybercrime, such as online fraud, extortion, identity theft, or illegal access to electronic systems.

These issues show that personal data protection is an important part of human rights protection in the digital era. The right to privacy is fundamentally a basic right closely related to individual dignity and freedom. At the international level, the right to privacy is recognized in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. In the Indonesian context, the guarantee of protection of one's person can also be linked to Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the protection of one's person, family, honor, dignity, and property under one's control. The development of digital technology has since expanded the meaning of this right, as personal information can now be collected and processed on a very large scale through electronic systems.

Recognition of the importance of personal data protection in Indonesia has been further strengthened by the enactment of Law Number 27 of 2022 on Personal Data Protection. The enactment of this law marks an important milestone in building a more comprehensive legal framework for personal data protection. The Personal Data Protection Law regulates the rights of personal data subjects, the obligations of personal data controllers and processors, the processing of personal data, the transfer of personal data, and provisions concerning administrative and criminal sanctions. With this regulation in place, personal data protection is no longer merely treated as a sectoral issue, but has become part of a more systematic national legal regime (Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, 2022).

In addition to the Personal Data Protection Law, regulations concerning electronic activities in Indonesia are also found in Law Number 11 of 2008 on Electronic Information and Transactions, as amended several times, including through Law Number 19 of 2016 and the second amendment through Law Number 1 of 2024. This legal framework provides the legal basis for regulating electronic information, electronic transactions, prohibited acts in the digital space, and law enforcement aspects concerning criminal acts involving electronic systems. In the context of information manipulation, regulations on electronic information are particularly relevant because certain forms of unlawful information dissemination may be subject to criminal provisions if they meet the elements set forth in the applicable legislation (Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, 2024).

Although the regulatory framework has developed, the effectiveness of legal protection for personal data and against information manipulation on social media still faces various challenges. The first challenge concerns legal substance. Digital technology develops very rapidly, while the formation and amendment of legislation requires a relatively long time. As a result, gaps often emerge between technological development and the law's ability to respond to new forms of violations. The development of artificial intelligence,

deepfakes, recommendation algorithms, and large-scale data collection technologies are examples of how technology can develop faster than the regulations governing it.

The second challenge concerns institutional and law enforcement aspects. Handling cybercrime requires technical capability and human resources with competence in digital forensics, information security, data analysis, and technology-based investigation. The cross-regional and even cross-border nature of cybercrime also raises jurisdictional issues and law enforcement coordination challenges. Perpetrators may be located in a different country from the victim or may use digital infrastructure spread across various jurisdictions. This condition makes the process of identifying perpetrators, collecting electronic evidence, and enforcing the law more complex (Wall, 2007).

The third challenge concerns the legal culture of society. The uneven level of digital literacy causes some social media users to not yet understand the risks arising from the use and dissemination of personal data. Many users still consider information such as phone numbers, addresses, identity photos, location, or family information to be ordinary information without strategic value. In fact, such information can be exploited by criminals to conduct profiling, phishing, social engineering, and identity theft. Therefore, personal data protection cannot rely solely on regulation and law enforcement officials, but also requires user awareness and responsibility in safeguarding personal data security.

From a cyber law perspective, the issues of personal data protection and information manipulation need to be understood as part of an interconnected digital security ecosystem. Data breaches can become a gateway for information manipulation, while information manipulation can use personal data as an instrument to construct false narratives or commit fraud. Thus, a legal approach that too rigidly separates personal data protection from information manipulation risks overlooking the causal and structural relationship between the two. An integrated approach is needed that can examine how data is collected, processed, used, and misused within the digital ecosystem.

Previous studies on privacy protection show that the development of information technology has created new challenges to the traditional concept of privacy. Solove (2006) explains that modern privacy issues relate not only to the disclosure of information but also encompass the collection, processing, use, and dissemination of personal information. This perspective is relevant to the development of social media because users often do not have full control over how their data is used after being submitted to a digital platform. Meanwhile, Nissenbaum (2010), through the theory of contextual integrity, emphasizes the importance of aligning information flow with social norms and context. In this perspective, a privacy violation can occur when information obtained in one context is used or disseminated in another context without adequate legitimacy.

Studies on information manipulation also show that social media has changed the character of information production and distribution. Wardle and Derakhshan (2017) affirm that the digital information ecosystem enables the emergence of various forms of false and manipulative information that can spread widely. This issue becomes increasingly complex because social media algorithms can amplify the spread of highly engaging content. Provocative or controversial information often receives greater

attention, giving it a higher chance of being widely disseminated. In this context, law enforcement needs to proceed hand in hand with increased digital literacy, platform transparency, and strengthened user protection mechanisms.

Based on these studies, it can be seen that research on personal data protection and information manipulation still has room for development. Some studies focus more on the aspect of personal data protection as part of privacy rights, while other studies focus on the spread of hoaxes and the application of criminal provisions in cyber law. In practice, however, these two issues are closely interrelated. Personal data can be used as material to produce information manipulation, while information manipulation can serve as a means to obtain or exploit personal data. Therefore, research is needed that examines both aspects in an integrated manner.

The novelty of this research lies in its effort to analyze the relationship between personal data protection and law enforcement against information manipulation on social media from the perspective of Indonesian cyber law. This research not only views personal data protection as a matter of privacy rights, but also examines how data misuse can contribute to the emergence of digital information manipulation. In addition, this research analyzes the effectiveness of the applicable regulatory framework by considering challenges in legal substance, law enforcement structure, and legal culture in society. With this approach, this research is expected to provide a more comprehensive understanding of the relationship between personal data protection, information security, and law enforcement in the digital space.

This research is relevant because society is increasingly dependent on social media as a means of communication, transactions, and obtaining information. This dependence makes personal data security and information integrity two inseparable aspects of legal protection in the digital era. The state has a responsibility to create regulations capable of providing legal certainty and protection for society, while digital platforms have a responsibility to implement security principles and data protection. At the same time, society also has a responsibility to increase digital literacy and safeguard the security of personal information.

Based on the description above, this research raises two problem formulations: first, what form does legal protection take for the personal data of social media users under Indonesian legislation? Second, how effective is law enforcement against information manipulation on social media from the perspective of Indonesian cyber law? The objectives of this research are to analyze the form of legal protection for the personal data of social media users based on the national legal framework, to examine the effectiveness of law enforcement against information manipulation on social media, and to identify various obstacles and strategic efforts in strengthening personal data protection and digital information security in Indonesia.

Theoretically, this research is expected to contribute to the development of legal scholarship, particularly in the fields of cyber law, personal data protection, privacy rights, and information technology-based crime. This research is also expected to enrich academic discourse regarding the relationship between personal data protection and

information manipulation within the social media ecosystem. Practically, the results of this research are expected to serve as considerations for the government in strengthening personal data protection regulations and policies, for law enforcement officials in improving their capacity to handle cybercrime, for electronic system operators in strengthening data security governance, and for society in raising awareness of the importance of personal data protection and the responsible use of social media. Thus, legal protection in the digital space is directed not only at taking action against violations, but also at building a digital ecosystem that is secure, trustworthy, transparent, and just.

## **METHOD**

This research employs a normative legal research method using both a statute approach and a conceptual approach. Normative legal research examines legal norms, legal principles, and various statutory regulations related to personal data protection and law enforcement against information manipulation on social media (Marzuki, 2017). The statute approach is used to analyze the legal provisions contained in Law Number 11 of 2008 on Electronic Information and Transactions as amended by Law Number 19 of 2016, as well as Law Number 27 of 2022 on Personal Data Protection. Meanwhile, the conceptual approach is used to understand the concepts of legal protection, privacy rights, and law enforcement from a cyber law perspective.

The legal materials used in this research consist of primary, secondary, and tertiary legal materials. Primary legal materials include statutory regulations related to personal data protection and cybercrime. Secondary legal materials consist of legal textbooks, scholarly journals, prior research findings, and academic articles relevant to the object of study. Tertiary legal materials include legal dictionaries, encyclopedias, and other supporting sources that help clarify legal terminology used in the research (Soekanto & Mamudji, 2015). Legal materials were collected through library research, examining various legal literature, official documents, and prior studies related to personal data protection and information manipulation on social media.

The analysis of legal materials in this research was conducted qualitatively using a descriptive-analytical method. This method involves describing and analyzing the applicable legal provisions concerning personal data protection and law enforcement against information manipulation on social media, then linking them to legal theories and legal facts developing in society (Sunggono, 2016). Through this method, the research is expected to produce a comprehensive understanding of the effectiveness of personal data protection and law enforcement against information manipulation from a cyber law perspective in Indonesia.

## **RESULT AND DISCUSSIONS**

### **LEGAL PROTECTION OF PERSONAL DATA OF SOCIAL MEDIA USERS UNDER INDONESIAN LEGISLATION**

The development of information and communication technology has brought major changes to society, particularly in the use of social media as a means of communication and information exchange. Social media allows every individual to access, store, and

disseminate information quickly without the limits of space and time. However, this development has also given rise to various legal issues, particularly concerning the protection of social media users' personal data. Personal data forms part of the right to privacy that must be protected because it is closely tied to individual identity and freedom. In practice, the use of social media is often accompanied by the collection and utilization of users' personal data by certain parties without valid consent, which has the potential to cause harm to the data owner. Legal protection of personal data is fundamentally a form of human rights protection guaranteed by the state. The right to privacy is a fundamental right inherent in every individual and forms an important part of life in modern society. Protection of personal data is needed to prevent data misuse, identity theft, information manipulation, and other forms of cybercrime. In the context of social media, users' personal data is often used for commercial, political, or illegal purposes that can harm society. Therefore, the state has an obligation to provide legal protection by establishing regulations capable of guaranteeing the security of society's personal data in the digital space.

Constitutionally, the protection of personal data can be linked to Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states that every person has the right to protection of their person, family, honor, dignity, and property under their control, as well as the right to a sense of security and protection from the threat of fear to do or not do something that constitutes a basic right. This provision shows that personal data protection is part of the protection of privacy rights guaranteed by the Constitution. Accordingly, any form of misuse of social media users' personal data constitutes a violation of citizens' constitutional rights. Before the enactment of Law Number 27 of 2022 on Personal Data Protection, regulation of personal data in Indonesia was scattered across various pieces of legislation, one of which was Law Number 11 of 2008 on Electronic Information and Transactions as amended by Law Number 19 of 2016 (Republic of Indonesia, 2016). Article 26 paragraph (1) of the Electronic Information and Transactions Law states that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. This provision affirms that every individual has the right to determine the use of their personal data in the digital space.

Legal protection of personal data under the Electronic Information and Transactions Law is essentially a form of preventive protection against the misuse of electronic information. Preventive protection is carried out by regulating the obligation to obtain the data owner's consent before personal data is used by other parties. In addition, the Electronic Information and Transactions Law also grants data owners the right to file a lawsuit in the event of a violation involving the use of personal data. This provision shows that the state provides a legal mechanism for the public to obtain protection and legal certainty when their privacy rights are violated. Nevertheless, the regulation of personal data protection under the Electronic Information and Transactions Law is considered not yet sufficiently comprehensive, as it only regulates the use of personal data in electronic media in general terms. This regulation does not yet provide a clear definition of the types of personal data, the rights of data owners, the obligations of data controllers, or the

mechanisms for enforcing the law against personal data violations. This condition has caused legal protection of social media users' personal data to not yet function optimally.

To strengthen legal protection of personal data, the government subsequently enacted Law Number 27 of 2022 on Personal Data Protection (Republic of Indonesia, 2022). The enactment of this law is an important step in creating a more comprehensive personal data protection system in Indonesia. Article 1 point 1 of the Personal Data Protection Law explains that personal data is data about an identified or identifiable individual, whether on its own or combined with other information, either directly or indirectly, through electronic or non-electronic systems. The Personal Data Protection Law provides more detailed regulation of the rights of personal data subjects. These rights include the right to obtain information regarding the clarity of the identity of the party requesting personal data, the right to complete and update personal data, the right to terminate the processing of personal data, the right to have personal data erased, and the right to claim compensation for violations of personal data. This regulation demonstrates a strengthening of legal protection for the public as owners of personal data.

In addition to protecting the rights of data owners, the Personal Data Protection Law also regulates the obligations of personal data controllers and personal data processors. Personal data controllers are obligated to maintain the confidentiality and security of the personal data they manage and are responsible for every processing activity carried out. In the context of social media, digital platforms as data controllers have an obligation to protect user data from illegal access, data breaches, and misuse by third parties. Another form of legal protection can also be seen in the administrative and criminal sanctions imposed for violations of personal data. Administrative sanctions may take the form of written warnings, temporary suspension of personal data processing activities, deletion of personal data, and administrative fines. Meanwhile, criminal sanctions are imposed on anyone who unlawfully obtains, discloses, or uses another person's personal data for certain purposes. These criminal provisions are intended to create a deterrent effect for perpetrators of personal data violations while also strengthening law enforcement in the field of personal data protection.

From a legal perspective, legal protection of personal data can be distinguished into preventive and repressive legal protection. Preventive protection is carried out through the establishment of regulations and supervision of the use of personal data, while repressive protection is carried out through law enforcement against personal data violations that have already occurred. Both forms of protection are essential in creating legal certainty and security for social media users in Indonesia. Although Indonesia already has specific regulations on personal data protection, the implementation of legal protection in practice still faces various obstacles. One of the main obstacles is the low level of public awareness regarding the importance of safeguarding personal data on social media. Many social media users voluntarily share personal information without understanding the risk of data misuse. In addition, weak digital security systems and inadequate oversight of social media platforms also mean that personal data breaches still frequently occur.

Another problem relates to the enforcement of the law against personal data violations, which remains ineffective. In practice, the process of enforcing the law against personal data violations often encounters obstacles, such as the difficulty of proving cybercrimes, the limited technological capacity of law enforcement officials, and the presence of perpetrators located outside Indonesia's jurisdiction (Wall, 2007). This condition shows that legal protection of personal data requires not only good regulation, but also readiness on the part of law enforcement officials and an adequate digital security system. Beyond the national legal aspect, personal data protection is also related to developments in international law. Many countries already have strict personal data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union (European Union, 2016). The enactment of the Personal Data Protection Law in Indonesia reflects an effort to harmonize national law with international standards on personal data protection. Through this harmonization, Indonesia is expected to be able to create a more effective personal data protection system capable of competing in the development of the global digital economy.

Thus, legal protection of the personal data of social media users in Indonesia has essentially been regulated through various pieces of legislation, particularly the Electronic Information and Transactions Law and the Personal Data Protection Law. This protection encompasses recognition of the public's right to privacy, the obligation to obtain consent for the use of personal data, the granting of rights to data owners to control the use of their data, and the imposition of administrative and criminal sanctions for personal data violations. Nevertheless, the effectiveness of this legal protection still requires strengthening in terms of law enforcement, public awareness, and oversight of the use of personal data on social media in order to create security and legal certainty in the digital space.

## **THE EFFECTIVENESS OF LAW ENFORCEMENT AGAINST INFORMATION MANIPULATION ON SOCIAL MEDIA FROM THE PERSPECTIVE OF CYBER LAW IN INDONESIA**

The effectiveness of law enforcement against information manipulation on social media is one of the central issues in the development of cyber law in Indonesia. This is due to the increasing intensity of social media use, which functions not only as a means of communication but also as an open space for the dissemination of information, including information that is false, misleading, or fabricated. From the perspective of cyber law, information manipulation is categorized as part of cybercrime, which can have a broad impact on social, political, and economic stability, and even on state security. Therefore, the effectiveness of law enforcement is an important indicator in assessing the extent to which the law is able to respond to the dynamics of such digital crime. Theoretically, the effectiveness of law enforcement can be measured through five main factors: legal substance, law enforcement officials, facilities and infrastructure, society, and legal culture (Soekanto, 1983). These five factors are interrelated in determining the success of law enforcement in the digital space. In the context of information manipulation on social media, the factor of legal substance relates to the extent to which existing regulations are able to accommodate technological developments and new types of crime. Meanwhile,

the factor of law enforcement officials relates to their technical capability and professionalism in handling cyber cases that are complex and cross-jurisdictional in nature.

From the aspect of legal substance, Indonesia already has several legal instruments used to take action against information manipulation, such as Law Number 11 of 2008 on Electronic Information and Transactions, which has been amended several times, and Law Number 1 of 2024 as the second amendment (Republic of Indonesia, 2024). The provisions of this law, particularly those concerning the dissemination of electronic information containing false or misleading news, form the primary basis for law enforcement against perpetrators of information manipulation on social media. In practice, however, these provisions are still often regarded as open to multiple interpretations and have not yet specifically regulated modern forms of information manipulation such as deepfakes, bot manipulation, and algorithmic disinformation. From the perspective of law enforcement officials, the effectiveness of handling information manipulation cases still faces various challenges. One of the main challenges is limited technical capability in identifying, tracing, and proving cybercrimes that are digital in nature and often involve perpetrators across national borders. In addition, the process of proof in information manipulation cases also requires specialized expertise in digital forensics, which is not yet fully possessed by all law enforcement officials. This condition causes law enforcement against information manipulation to often proceed slowly and less than optimally.

Furthermore, from the aspect of facilities and infrastructure, the effectiveness of law enforcement is also influenced by the availability of supporting technology, such as digital tracking systems, data analysis tools, and cybersecurity infrastructure. In many cases, these facility limitations prevent the investigative process from being carried out to its full potential. In cybercrime, however, speed and accuracy in collecting digital evidence are decisive factors in the success of the legal process. From the societal aspect, low digital literacy is a hindering factor in the effectiveness of law enforcement against information manipulation on social media. Many social media users are not yet able to distinguish between accurate information and information that has been manipulated. In addition, a culture of "sharing without verification" also accelerates the spread of false information, thereby worsening the impact of information manipulation in the digital space. In this context, the public is not only a victim but also often becomes part of the spread of manipulated information.

Meanwhile, from the aspect of legal culture, there remains a tendency among the public to prefer resolving disputes through social media rather than through formal legal channels. This shows that public legal awareness of the importance of legal protection in the digital space still needs to be improved. This still-weak legal culture contributes to a low rate of reporting and formal legal handling of information manipulation cases. From the perspective of cyber law, information manipulation is not only viewed as a violation of national law but also as part of a global challenge. This is due to the borderless nature of the internet, which allows perpetrators to easily commit crimes from various countries without being bound by any particular jurisdiction (Wall, 2007). This condition demands

international cooperation in cyber law enforcement, including in the exchange of information, extradition of perpetrators, and harmonization of regulations between countries. In addition, the development of artificial intelligence technology further complicates efforts to enforce the law against information manipulation. Technologies such as deepfakes and content-distribution algorithms enable the production of highly realistic false information that is difficult to distinguish from genuine information. This poses a new challenge for law enforcement officials in carrying out verification and proof in court. Overall, the effectiveness of law enforcement against information manipulation on social media in Indonesia remains suboptimal. This is evident from the still-high rate of dissemination of false information, the limited capacity of law enforcement officials, and the not-yet-maximal implementation of existing regulations. Although Indonesia already has a fairly strong legal basis, implementation on the ground still faces various structural and cultural obstacles that affect the effectiveness of law enforcement. Therefore, more adaptive regulatory strengthening is needed in response to digital technological developments, along with increased capacity of law enforcement officials in the field of information technology and improved public digital literacy. In addition, cooperation among the government, social media platforms, and the public is also an important factor in creating a digital ecosystem that is safe and free from information manipulation.

Beyond the factors described above, the effectiveness of law enforcement against information manipulation on social media is also greatly influenced by the rapid pace of digital technological development. The increasingly complex changes in patterns of cybercrime often cause the law to lag behind technology. In this context, information manipulation no longer takes the simple form of spreading false news, but has developed into more sophisticated forms, such as deepfakes, manipulation of content-distribution algorithms, and the use of artificial intelligence to produce and disseminate false information on a massive and structured scale. This condition demands legal reform that is adaptive and responsive to technological development. In law enforcement practice, one of the main challenges is proof in information manipulation cases on social media. The system of proof in Indonesian criminal procedural law still relies heavily on conventional forms of evidence, whereas cybercrime requires a digital approach to proof based on digital evidence. Digital evidence has characteristics that make it easy to alter, delete, or manipulate, thus requiring sophisticated digital forensic techniques to ensure its validity and authenticity. This poses a serious challenge for law enforcement officials in ensuring that evidence presented in court can genuinely be scientifically and legally accounted for.

On the other hand, the effectiveness of law enforcement is also greatly influenced by coordination among law enforcement institutions. Handling cases of information manipulation on social media involves not only the police, but also requires cooperation with the prosecutor's office, the courts, and ministries or agencies with authority in the field of information and communication technology. A lack of effective coordination among institutions often causes the case-handling process to become slow and inefficient. In addition, differing understandings of the characteristics of cybercrime among law

enforcement officials can also affect the quality of case handling. From a regulatory perspective, although the Electronic Information and Transactions Law provides a legal basis for handling information manipulation, considerable room for interpretation remains in its application. For example, the terms "misleading information" or "false news" often give rise to debate in legal practice because they do not always have clear boundaries. This lack of clarity in the norms has the potential to create legal uncertainty and may open the door to the criminalization of freedom of expression if not applied carefully. In addition, the development of social media platforms operated by global technology companies presents its own challenge to law enforcement in Indonesia. Much of the data and many of the servers of social media platforms are located outside Indonesia's jurisdiction, making the process of evidence collection and cross-border law enforcement more difficult. In this context, stronger international cooperation is needed through mechanisms such as mutual legal assistance, as well as the harmonization of data protection and cybercrime regulations between countries.

Another equally important aspect is the role of social media platforms themselves as intermediary service providers. Platforms bear responsibility for moderating content and preventing the spread of manipulative information. In practice, however, content moderation mechanisms are often not yet optimal due to the very large volume of content and the limitations of algorithms in detecting the context of information. Therefore, stronger regulation is needed to more firmly define platform responsibility in preventing and taking action against the spread of manipulated information. In addition, the effectiveness of law enforcement also depends heavily on public participation in reporting and identifying information suspected of being manipulative. Without active public participation, law enforcement efforts will not function optimally. However, low digital literacy means that many members of the public are unaware that they are dealing with information that has been manipulated. This shows that legal education and digital literacy play a very important role in supporting the effectiveness of law enforcement in the digital era.

From the perspective of cyber law, law enforcement should not be solely repressive in nature but must also prioritize preventive and educational approaches. The preventive approach is carried out through strict regulation, oversight of digital platforms, and strengthening of data security systems. Meanwhile, the educational approach is carried out by improving public digital literacy so that people are able to recognize, filter, and understand the information circulating on social media. Thus, law enforcement should focus not only on punishing perpetrators, but also on preventing cybercrime from occurring in the first place. Overall, the effectiveness of law enforcement against information manipulation on social media in Indonesia still faces various multidimensional challenges, whether from the legal, technological, institutional, or social aspects. Although the legal instruments are already in place, their implementation still requires significant strengthening in order to respond to the increasingly complex challenges of cybercrime. Therefore, synergy is needed among the government, law enforcement officials, digital platforms, and the public to create a digital ecosystem that is safe, transparent, and accountable.

## CONCLUSIONS

The development of information and communication technology has had a significant impact on society, particularly in the use of social media, which functions not only as a means of communication but also as a space vulnerable to legal violations. The issues of personal data protection and information manipulation have become major concerns in Indonesian cyber law because they are directly related to privacy rights, individual security, and social stability. Personal data, as part of human rights, is often misused in various forms, such as identity theft, the dissemination of hoaxes, and information manipulation, which can harm both individuals and society at large. Therefore, the state has a responsibility to provide comprehensive legal protection through applicable regulations. Legal protection of personal data in Indonesia is regulated through the Electronic Information and Transactions Law and the Personal Data Protection Law, which provide a legal basis for protecting the privacy rights of social media users. These regulations cover the recognition of data subject rights, the obligations of data controllers, and administrative and criminal sanctions for personal data violations. Nevertheless, the implementation of such legal protection continues to face various challenges, including low levels of digital literacy among the public, limited oversight, and the lack of optimal law enforcement against personal data violations in the digital sphere.

Law enforcement against information manipulation on social media from the perspective of cyber law in Indonesia remains less than optimal. This is attributable to various factors, including limitations in the existing legal framework, which has not fully accommodated emerging technologies such as deepfakes and artificial intelligence; limited digital forensics capabilities among law enforcement authorities; and weak coordination among law enforcement agencies. In addition, societal factors and legal culture also affect the effectiveness of law enforcement, particularly low levels of legal awareness and digital literacy, which contribute to the widespread dissemination of unverified information. Global challenges, such as the borderless nature of the internet, the involvement of international digital platforms, and the complexity of digital evidence, further complicate law enforcement efforts against information manipulation. Therefore, it is necessary to strengthen regulations so that they can adapt to technological developments, enhance the capacity of law enforcement authorities, and improve public digital literacy. Synergy among the government, law enforcement agencies, digital platforms, and society is a key factor in establishing an effective legal protection system in the digital era.

## BIBLIOGRAPHY

American Civil Liberties Union. (2022). *Privacy and technology*. ACLU.

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union.

- Marzuki, P. M. (2017). *Penelitian hukum* [Legal research]. Kencana.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Republic of Indonesia. (2016). *Law Number 19 of 2016 on the Amendment of Law Number 11 of 2008 on Electronic Information and Transactions*.
- Republic of Indonesia. (2022). *Law Number 27 of 2022 on Personal Data Protection*.
- Republic of Indonesia. (2024). *Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions*.
- Soekanto, S. (1983). *Faktor-faktor yang mempengaruhi penegakan hukum* [Factors influencing law enforcement]. Rajawali Pers.
- Soekanto, S., & Mamudji, S. (2015). *Penelitian hukum normatif: Suatu tinjauan singkat* [Normative legal research: A brief overview]. Rajawali Pers.
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–560.
- Sunggono, B. (2016). *Metodologi penelitian hukum* [Legal research methodology]. Rajawali Pers.
- United Nations. (1948). *Universal Declaration of Human Rights*. United Nations.
- United Nations. (1966). *International Covenant on Civil and Political Rights*. United Nations.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe.