Indonesian Journal of Education and Social Humanities

Indonesian Journal of Education and Social Humanities
Volume 2 (2) June 2025
ISSN: 3047-9843
The article is published with Open Access at: https://journal.mgedukasia.or.id/index.php/ijesh

Digital Communication Ethics in Law Enforcement in the Community Environment

Dini Anggraini ✉, Universitas Malikussaleh, Indonesia
Dwi Fitri, Universitas Malikussaleh, Indonesia
Nurul Munira, Universitas Malikussaleh, Indonesia
Fani Aprilia, Universitas Malikussaleh, Indonesia
Melisa Ariani, Universitas Malikussaleh, Indonesia
Siti Nazwa, Universitas Malikussaleh, Indonesia
Bella Aldama, Universitas Malikussaleh, Indonesia
Julinda, Universitas Malikussaleh, Indonesia
Zaki Ryan Saputra, Universitas Malikussaleh, Indonesia

✉ *dini.230240046@mhs.unimal.ac.id*

Abstract: The rapid development of digitalization has brought significant changes to all aspects of life, especially the way humans communicate and law enforcement. As a widespread and interactive digital platform, social media provides a space for people to express themselves publicly. However, this freedom also brings new challenges, such as the spread of misinformation, hate speech, and defamation, which often result in legal action. In Indonesia, regulations regarding digital communication practices are mainly regulated through the Electronic Information and Transactions Law (UU ITE). Although the law is an important tool for maintaining social order, its implementation often triggers debate about the balance between protecting freedom of expression and the state's obligation to maintain social order. This article discusses the ethics of digital communication in the context of law enforcement, emphasizing the balance between protecting individual privacy and the public interest. The author discusses the various challenges faced in the implementation of the Electronic Information and Transactions Law (UU ITE) and considers its impact on human rights, especially in terms of freedom of expression and personal data protection. On the one hand, individuals have the right to maintain their privacy; on the other hand, the state has an obligation to maintain public security and control the spread of information that can disrupt public order. In this way, this article is expected to enrich the understanding of the dynamics of digital communication ethics in the legal field and provide input for better policy making in the future.

Keywords: Digital communication ethics, law enforcement, freedom of expression, privacy, UU ITE.

Received Macrh 6, 2025; **Accepted** May 15, 2025; **Published** June 23, 2025

Published by Mandailing Global Edukasia © 2025.
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

INTRODUCTION

The digital revolution has fundamentally changed the way humans communicate. Today, social media platforms such as Twitter, Facebook, Instagram, and TikTok are not only tools for sharing information, but also new public spaces for discussion, advocacy, and social

criticism. These changes have brought many benefits, but also significant challenges, especially related to jokes, hate speech, cyberbullying, and privacy violations. In this context, digital space has become a dynamic realm that on the one hand encourages the development of freedom of speech, but on the other hand is also vulnerable to misuse and can have legal consequences. The government has responded to this development by enacting laws and regulations such as the Electronic Information and Transactions Law (UU ITE) which aims to regulate user behavior in the digital world. However, the implementation of the ITE Law has been repeatedly criticized. Some believe that the implementation of the law is often ambiguous and can limit the basic rights of citizens, especially freedom of speech. A study conducted by Kusumo et al. (2021) revealed that many reported cases of defamation were actually related to the expression of opinions that should be protected in a democratic country. This situation raises an ethical dilemma about how to balance law enforcement and human rights protection in the digital space.

The government has responded to this development by enacting laws and regulations such as the Electronic Information and Transactions Law (UU ITE) which aims to regulate user behavior in the digital world. However, the implementation of the ITE Law has been repeatedly criticized. Some believe that the implementation of the law is often ambiguous and can limit the basic rights of citizens, especially freedom of speech. A study conducted by Kusumo et al. (2021) revealed that many reported cases of defamation were actually related to the expression of opinions that should be protected in a democratic country. This situation raises an ethical dilemma about how to balance law enforcement and human rights protection in the digital space.

As society's dependence on information technology continues to increase, concerns about privacy issues are also increasing. Bahram (2023) highlights that in the digital ecosystem, information manipulation and social engineering practices can endanger individual sovereignty, as personal data is often used for political or commercial interests without consent. On the other hand, Wulandari (2023) argues that privacy protection should not be seen as an obstacle to the public interest, but rather as a fundamental element of human rights that must continue to be upheld, including in the context of law enforcement. In this context, digital communication ethics is an important aspect that must be taken seriously. This ethics not only concerns individual behavior in the digital space, but also how the state and law enforcers treat their citizens in cyberspace. Transparency, impartiality, and accountability are the main principles of fair and balanced law enforcement in the era of digital communication. Against this backdrop, this article aims to provide an in-depth analysis of the dynamic relationship between digital communication ethics and law enforcement, focusing on three main issues, namely the protection of personal privacy, transparency of legal mechanisms, and the balance between public interest and freedom of expression. By reviewing various academic literature and relevant case studies, this paper hopes to contribute to building a more ethical digital communication ecosystem that supports democratic principles.

Digital communication is a form of interaction through electronic media based on the internet network that allows the exchange of information quickly and on a large scale without geographical boundaries. Bahram (2023) stated that digital communication is not only a means of exchanging information, but also a means of social engineering that can shape, guide, and even manipulate public opinion through digital platform algorithms. Therefore, the application of ethics in digital communication is very important. Digital communication ethics refers to a series of moral values that govern the behavior of individuals and institutions when they interact in cyberspace. Basic principles such as honesty, responsibility, fairness and respect for privacy are the main foundations of this communication activity. For example, honesty requires everyone to avoid spreading false or misleading information, while responsibility involves awareness of the consequences of every upload, comment, or other form of communication on others and society as a whole.

In the context of law enforcement, digital communication ethics has a more complex dimension. Not all forms of ethical violations can be regulated by law, but every ethical

violation has the potential to cause legal problems, especially when it comes to the spread of defamation, defamation, or personal data violations. That is why it is very important to build a strong culture of digital literacy in your community. Febriyanti and Zubaedi (2023) stated that moral literacy in the digital world does not only refer to technical skills in using technology, but more deeply to the ability to understand the social and ethical implications of online communication behavior.

The application of digital communication ethics also needs to pay attention to cultural diversity and local values. For example, standards of politeness in communication may differ in each community, so communicators in the digital world must be sensitive to culture. Globally, international ethical standards such as the United Nations Declaration of Human Rights, which emphasizes freedom of expression and protection of privacy, should be the main reference for interactions in cyberspace. One of the main challenges in implementing digital communication ethics is anonymity on the internet, which often gives rise to unethical behavior such as trolling, doxing, and cyberbullying, which are difficult to identify and prosecute under the law. Therefore, digital ethics should not only be understood as normative rules, but also built as a shared awareness of the digital community.

The Electronic Information and Transactions Law (UU ITE) in Indonesia was drafted as an effort to respond to rapid developments in the field of information and communication technology. Initially, Law No. 11 of 2008 was intended to provide legal certainty for various digital activities, such as electronic transactions, personal data protection, and information security. Over time, the scope of the ITE Law has also expanded to regulate individual expression in cyberspace, especially in cases of insults, defamation, the spread of fake news, and hate speech. Kusumo and colleagues (2021) noted that although the main objective of this law is to maintain order and security in the digital space, its implementation is often controversial. Many people argue that several articles, such as Article 27 paragraph (3) concerning defamation and Article 28 paragraph (2) concerning hate speech based on SARA, contain ambiguous interpretations. As a result, these articles are often used to limit criticism, social movements, and political expression that are actually protected. Freedom of expression itself is a fundamental right guaranteed in the Indonesian constitution through Article 28E paragraph (3) of the 1945 Constitution, as well as in various international conventions such as the International Covenant on Civil and Political Rights (ICCPR), which has been ratified by Indonesia.

However, this right is not absolute. There are limitations that apply, especially if the expression threatens national security, public order, or the human rights of others. The main challenge is how to interpret these limitations fairly and not excessively. In Indonesia, this imbalance is often clearly visible. Syahril and colleagues (2022) noted an increasing trend in the criminalization of criticism on social media directed at public officials or state institutions, on the grounds of violating the ITE Law. This phenomenon not only threatens the principles of digital democracy, but also creates a deterrent effect (chilling effect) in society, where individuals become reluctant to voice critical opinions for fear of getting caught up in legal problems.

It is important to realize that law enforcement against digital expression must be based on the principles of caution, proportionality, and accountability. As proposed by Febriyanti and Zubaedi (2023), the revision of the ITE Law needs to provide clarity on the previously ambiguous legal definitions, limit the use of criminal law as a last resort (ultimum remedium), and strengthen alternative dispute resolution mechanisms, such as mediation. Globally, the legal approach to freedom of expression in the digital world emphasizes the principle of "legitimate purpose and absolute necessity," where restrictions can only be applied for legitimate purposes and are truly necessary in a democratic society. Therefore, Indonesia is expected to reform its digital regulations to comply with international human rights standards, while maintaining order in the digital space in a fair and democratic manner.

In the digital era, the right to privacy has become an important issue that has received great attention in discussions on communication law and ethics. Privacy is not only related to the protection of personal data, but also includes individual control over their personal information, including how, when, and with whom the information is shared. In the context of law enforcement, the right to privacy often conflicts with the public interest, especially when the state seeks to access personal data for reasons of national security, crime prevention, or law enforcement. According to Wulandari (2023), digital privacy must be viewed as a basic right inherent in every individual, in line with the principles of human rights.

Violations of privacy without a legitimate reason not only damage public trust in state institutions, but also threaten freedom of expression, innovation, and citizen participation in democratic life. On the other hand, in certain situations, the state does have justification to limit privacy, for example to protect public security or enforce the law against illegal acts. The conflict between the right to privacy and the public interest is a major challenge in the formulation of digital communication policies and cyber law. On the one hand, the public demands stronger data protection, especially after the many cases of personal data leaks in Indonesia. On the other hand, the state feels the need to monitor digital space to prevent threats such as terrorism, the spread of hoaxes, or hate speech that can divide society. An ethical approach to this problem requires the application of the principles of transparency, accountability, and proportionality. As expressed by Gede et al. (2023), law enforcement officers' access to personal data must be based on clear regulations, supervised by an independent institution, and through fair legal procedures, such as obtaining permission from the court (judicial warrant).

In addition, there must be restrictions on the scope and duration of data access to prevent potential abuse of power. Privacy and the public interest should not be viewed as two things that are always in conflict, but as two values that need to be balanced. In many situations, the public interest can be protected without having to sacrifice privacy excessively. For example, instead of conducting mass surveillance, the state can adopt a more focused intelligence approach based on real risks. In addition, civil society plays a crucial role in overseeing policies related to digital privacy. Public advocacy, independent media, and non-governmental organizations need to be involved in designing, implementing, and evaluating data protection policies. Only in this way can a balance between individual rights and public interests be achieved in a fair and civilized manner in Indonesia's digital ecosystem.

METHODS

This study uses a literature study approach to analyze various sources related to digital communication ethics, law enforcement in the digital space, and the implementation of the ITE Law in Indonesia. This approach allows for a comprehensive analysis of various expert perspectives and current issues.

RESULTS AND DISCUSSION

Digital Communication Practices in Law Enforcement

Digital communication has revolutionized the public sphere, enriching democracy by providing new platforms for expression and advocacy. However, it also presents novel legal challenges, such as the spread of hoaxes and hate speech. Many legal cases now originate from online activities, often involving controversial interpretations of the Electronic Information and Transactions Law (UU ITE), particularly articles concerning defamation and the dissemination of false information (Syahril et al., 2022). There exists a tension between freedom of expression and the protection of reputation and public order. Law enforcement in the digital realm requires caution to avoid criminalizing constitutionally

protected expression. Law enforcement officers face challenges in objectively assessing digital content, especially due to low digital literacy. Understanding the context of digital communication is crucial for accurate and proportional judgment (Febriyanti & Zubaedi, 2023). The principle of due process must also be upheld, ensuring that all legal procedures are fair, transparent, and accountable.

Nevertheless, law enforcement in the digital space remains essential to combat cybercrimes such as fraud and the spread of hate speech. Balancing the maintenance of order with the respect for human rights must be prioritized. An effective approach requires enhancing the digital literacy of law enforcers, ongoing training on the characteristics of the digital environment, and regulatory reforms aligned with international human rights standards related to freedom of expression. The goal is effective, fair law enforcement that does not foster excessive fear within society.

Ethics in the Law Enforcement Process

Law enforcement in the digital domain demands profound ethical considerations to balance the state's obligation to maintain order with citizens' fundamental rights, especially freedom of expression and privacy protection. Failure to apply ethical principles can lead to injustice, excessive criminalization, and loss of public trust in the judicial system. Therefore, ethical principles such as transparency, accountability, objectivity, and proportionality must form the foundation of the digital law enforcement process. Transparency requires openness of legal processes to the public, including access to information about the legal basis and evidence used to designate suspects. This is vital to prevent abuse of power and encourage public oversight. Accountability ensures that every action by law enforcement officers is responsible and auditable, guaranteeing a fair legal process.

Objectivity demands unbiased assessment of digital content, focusing on the substance rather than the content creator’s identity. Proportionality emphasizes the importance of considering the level of harm caused before legal action, avoiding the criminalization of protected criticism or expression. Protection of personal data is a critical aspect. Data access must be minimal and through legitimate legal channels to prevent abuse. Robust regulations and supervision are necessary to ensure privacy protection (Febriyanti & Zubaedi, 2023; Bahram, 2023; Wulandari, 2023). Restorative approaches, such as education or mediation, may serve as alternatives to criminal penalties for minor violations. The establishment of specialized cybercrime units prioritizing ethics and human rights, with an educational role, is highly recommended. Ethics must be the primary guideline, ensuring that digital security does not come at the cost of freedom of expression. Fair and proportional law enforcement in the digital world requires strong commitment to ethical principles and human rights protection.

The Role of Media and Civil Society

Media and civil society organizations play a vital role in maintaining the balance between freedom of expression and law enforcement in the digital realm. Both act as a counterbalance to state authority in upholding order and protecting civil rights within a democratic system. Media independence and the critical stance of civil society are crucial to prevent abuse of authority in digital law enforcement that could silence public opinion or restrict free speech.

Firstly, the media is responsible for verifying information and ensuring the accuracy of news circulating in the digital space. In an era of rapid and widely disseminated information, verification poses a significant challenge; nevertheless, media must serve as the first line of defense against hoaxes and disinformation that can undermine social and political stability (Rizki & Widodo, 2023). Moreover, the media needs to apply principles of balance when delivering information, especially on sensitive or controversial issues that may lead to legal processes. Media also play a role in public education regarding digital

ethics and the legal consequences of digital space misuse through various platforms such as articles, interviews, and campaigns. Thus, media not only convey information but also shape public legal awareness.

Civil society, especially NGOs focused on human rights, freedom of expression, and data protection, play a role in monitoring and evaluating policies and practices of digital law enforcement. They serve as the frontline defenders against legal abuse to suppress freedom of expression. For example, some NGOs in Indonesia actively critique provisions in the UU ITE considered restrictive toward freedom of opinion, particularly concerning hate speech and defamation (Syahril et al., 2022). Civil society also advocates legal reforms, ensuring that laws like the UU ITE align with human rights principles. They strive to prevent laws from being misused for political or business interests and advocate for stricter personal data protection to prevent misuse that harms individuals and restricts freedom of expression. Such efforts are carried out through campaigns, research, and legal advocacy.

Collaboration among media, civil society, academics, and the government is crucial to crafting public policies responsive to digital challenges. Open and transparent discussions about privacy, freedom of expression, and technology misuse will yield fairer and wiser policies. Media and civil society, as watchdogs and key actors, contribute to building a healthy, safe, and democratic digital ecosystem where individuals' rights to communicate and express themselves are protected.

CONCLUSION

Digital communication ethics in law enforcement is a complex issue involving legal, social, moral, and political dimensions. This study examines the challenges in regulating digital communication in Indonesia, especially related to the implementation of the Electronic Information and Transactions Law (UU ITE). The development of digital technology has expanded freedom of expression, but has also given rise to problems such as the spread of hoaxes and violations of privacy. The ITE Law, although important, often creates a dilemma between protecting individual rights and the public interest; disproportionate law enforcement can limit freedom of expression. Therefore, a balanced approach is needed, protecting privacy while guaranteeing freedom of opinion. This analysis shows that digital communication ethics in law enforcement must be based on the principles of justice, transparency, and accountability. The state needs to balance law enforcement with respect for citizens' rights. Law enforcement in the digital space requires caution so as not to hinder democracy. Law enforcement officers need adequate digital literacy and understanding of human rights. Civil society and the media have an important role in monitoring and criticizing policies related to digital communication. Responsible journalism and public participation strengthen social control. Therefore, periodic evaluation and updating of the ITE Law are needed to keep up with technological developments and the needs of society. Responsive legal reform and collaboration between government, civil society and academia are essential to creating a healthy, ethical and fair digital environment for all parties.

REFERENCES

Bahram, M. (2023). Tantangan hukum dan etika (rekayasa sosial terhadap kebebasan berpendapat di dunia digital). SENTRI: Jurnal Riset Ilmiah, 2(12), 5092-5109.

Kusumo, V. K., Junia, I. L. R., Prianto, Y., & Ruchimat, T. (2021). Pengaruh UU ITE terhadap kebebasan berekspresi di media sosial. Prosiding Senapenmas, 1069.

Febriyanti, I. H., & Zubaedi, D. (2023). Etika komunikasi di era digital dalam konteks hukum. Selasar: Jurnal Komunikasi dan Sosial Humaniora, 5(2), 22–34.

Gede, I. A. P., et al. (2023). Reformulasi hukum dalam era disrupsi digital. JAH: Jurnal Administrasi Hukum, 5(1), 15–27.

Syahril, M., et al. (2022). Kebebasan berekspresi dalam media sosial dan penerapan UU ITE. Journal Publicuho, 7(3), 102–118.

Pradana, H. A. (2023). Komunikasi digital pada masyarakat adat: Studi kasus penyebaran informasi hukum. Indigenous: Jurnal Ilmiah Komunikasi, 8(1), 44–59.

Taufik, M. (2023). Etika komunikasi digital dalam kebijakan publik. JHCJ: Jurnal Hukum dan Civil Justice, 7(2), 301–315.

Agustina, S., Fitri, D., & Muzaffarsyah, T. (2024). Strategi Komunikasi Pemerintah Dalam Mensosialisasikan Program Website Layanan Aspirasi Dan Pengaduan Online Rakyat (Lapor) Di Kota Padangsidimpuan. Cendekia: Jurnal Hukum, Sosial Dan Humaniora, 2(1), 434-446.

Rizki, F. A., & Widodo, B. (2023). Kritik sosial melalui media digital dan tantangan hukum. JAHE: Jurnal Administrasi dan Hukum Ekonomi, 6(1), 88–97.

Usman, & Devi, S. A. (2025) Etika Berkomunikasi dalam Pandangan Hukum Pidana Islam. Jurnal Penelitian Multidisiplin dalam Ilmu Pengetahuan, Teknologi, dan Pendidikan, 2(2), 3130-3134.

Purwatiningsih, D., Lestari, T., & Sulistyowati, Y. (2020). Etika Komunikasi di Media Sosial. Jurnal Komunikasi: Teori dan Praktik, 18(2), 123-132.

Arifah & abdul rahman ashidiq (2024). "Aspek hukum dan tantangan etika jurnalistik dalam penyebaran konten viral di era digital (studi di kabupaten toboali, bangka selatan)". JSIM: jurnal ilmu sosial dan pendidikan p-ISSN: 2721-2491 e-ISSN: 2721-2246 vol.5, No.4

Larasati, A. K., Widyaningsih, A., & Aryanto, C. A. (2023). Keterlibatan Hukum dan Etika di Era Internet. Indigenous Knowledge, 2(3), 158-164.

Dina marliana & muhammad ihsan syahputra (2024). "Etika komunikasi dalam penyiaran konten selebritis di program insert trans tv di era digital". Jurnal Penelitian Inovatif (JUPIN) Vol. 4, No. 1, Hal. 29-40 p-ISSN: 2808-148X e-ISSN: 2808-1366.

Hotma P. Sibuea, Diana Fitriana "PENYULUHAN HUKUM ETIKA DIGITAL BAGI PENGGUNA MEDIA SOSIAL DI SMK 01 PELAYARAN MUNDU, CIREBON" Empowerment: Jurnal Pengabdian Masyarakat, e-ISSN 2598-2052 Vol. 05 Nomor 03. 2022.248-257.