

The Paradox of Technological Progress and the Ethical Crisis in Digital Civilization

Nopit Ernasari^{1*}, Naib¹, Adithya Tri Firmansyah¹

¹ Faculty of Law, Pamulang University, Indonesia

*Corresponding Author Email: dosen02988@unpam.ac.id

Article History: Received: May 29, 2026; Accepted: July 18, 2026

ABSTRACT

The advancement of digital technology has significantly transformed various aspects of human life while creating new opportunities for increasingly sophisticated cybercrime. This phenomenon reflects an ethical crisis in digital civilization, characterized by declining moral responsibility in the use of digital technology. Although cybercrime has been widely examined from technological and criminal law perspectives, limited attention has been given to integrating digital ethics, digital literacy, and legal responses into a comprehensive preventive framework. This study aims to analyze the relationship between digital technological advancement and the emergence of cybercrime as a manifestation of this ethical crisis, as well as to examine preventive strategies through law enforcement, digital ethics, and digital literacy. This research employs normative legal research with a descriptive qualitative approach. Data were collected through library research, including legislation, books, scholarly journals, and official documents, and were analyzed using qualitative content analysis. The findings reveal that digital technology has improved efficiency and access to information while facilitating hacking, data theft, online fraud, malware distribution, and privacy violations. These developments demonstrate that technological progress without ethical awareness may undermine trust and security in the digital environment. The study's novelty lies in proposing an integrated legal framework that combines adaptive law enforcement, digital ethics, and digital literacy as complementary strategies for cybercrime prevention. Its main legal contribution is the development of a normative approach that strengthens preventive legal policies beyond conventional punitive measures. The findings also provide practical guidance for policymakers, law enforcement agencies, educational institutions, and digital stakeholders in fostering a secure, ethical, and sustainable digital ecosystem.

Keywords: Cybercrime, Digital technology, Digital ethics, Digital literacy, Cyber law.

1. INTRODUCTION

Human civilization has continuously evolved alongside the advancement of science and technology. The digital revolution has become a defining milestone, fundamentally transforming the ways people communicate, work, conduct transactions, and access information. The Internet, artificial intelligence (AI), cloud computing, the Internet of Things (IoT), and big data technologies have collectively shaped an increasingly interconnected digital environment that is deeply embedded in everyday life. According to the Digital 2025 Global Overview Report published by We Are Social and Meltwater, the global number of Internet users has reached approximately 5.56 billion, representing nearly 68% of the world's population, while social media users exceed 5.24 billion. These figures indicate that digital space has evolved into a new social sphere that profoundly influences nearly every dimension of human life (We Are Social, 2025).



Indonesia has likewise experienced rapid digital transformation. Data released by the Indonesian Internet Service Providers Association (APJII) in 2024 show that Internet penetration has reached approximately 79.5% of the national population, equivalent to more than 221 million Internet users (APJII, 2024). This transformation has generated substantial benefits, including improved economic productivity, broader access to information, enhanced public services, and accelerated innovation across multiple sectors. Nevertheless, this progress has also revealed a paradox: technological advancement has not necessarily been accompanied by corresponding moral and ethical development.

From a philosophical perspective, technology is fundamentally value-neutral. Heidegger (1977) argued that technology is not merely an instrument but also a mode through which human beings interpret and shape reality. Consequently, the impact of technology depends largely on the ethical principles and values that govern its use. When technological progress outpaces society's moral development, digital space ceases to function solely as a medium for collective advancement and instead becomes a platform for the abuse of power, information manipulation, data exploitation, and various forms of cybercrime. In this context, cybercrime should not be viewed merely as a technical or legal issue but rather as a manifestation of an ethical crisis within digital civilization (Heidegger, 1977).

This phenomenon is reflected in the growing prevalence of cybercrime at both global and national levels. According to the Internet Crime Report 2024 published by the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), cybercrime causes financial losses amounting to billions of U.S. dollars annually, with increasing cases involving phishing, identity theft, ransomware, online fraud, and data breaches (Yarbrough, 2024). Similarly, Indonesia's National Cyber and Crypto Agency (BSSN) regularly reports millions of anomalous cyber activities and cyberattacks targeting strategic sectors across the country. These developments demonstrate that digital technological advancement has created broader opportunities for increasingly sophisticated, transnational, and difficult-to-detect cybercrimes.

The increasing prevalence of cybercrime reflects a growing imbalance between technological advancement and the development of digital ethics. The freedom enabled by digital technologies is often not accompanied by an adequate sense of moral responsibility. As a result, digital environments have become increasingly vulnerable to misinformation, hate speech, digital fraud, personal data theft, unauthorized access to electronic systems, and digital identity exploitation. These conditions illustrate that technological progress without ethical foundations may erode human values, social trust, and security in the digital environment. This issue



constitutes the central focus of the present study, which examines how digital technological advancement influences the emergence and evolution of cybercrime as a manifestation of the ethical crisis in digital civilization.

At the same time, the complexity of cybercrime cannot be effectively addressed solely through repressive legal enforcement. Cybercrime evolves rapidly alongside technological innovation, causing legal frameworks to frequently lag behind emerging criminal methods. Accordingly, a more comprehensive approach is required through strengthened legal regulation, enhanced institutional capacity for law enforcement agencies, digital ethics education, and improved public digital literacy. In Indonesia, the enactment of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (EIT Law), Law Number 27 of 2022 on Personal Data Protection, and the implementation of the National Cybersecurity Strategy represent significant milestones toward establishing a more secure digital governance framework. Nevertheless, the effectiveness of these legal instruments ultimately depends on the development of a digital culture grounded in ethical awareness and moral responsibility.

Based on these considerations, this study is significant because it not only examines the relationship between digital technological advancement and the increasing prevalence of cybercrime as a reflection of the ethical crisis in digital civilization but also analyzes strategies for addressing these challenges through legal enforcement, the promotion of digital ethics, and the enhancement of digital literacy. Through this comprehensive approach, the study seeks to formulate strategies capable of fostering a secure, ethical, and responsible cyberspace, ensuring that technological advancement serves as a means of strengthening human civilization rather than becoming a threat to the very values upon which that civilization depends.

2. RESEARCH METHOD

This research constitutes a normative legal study. Within the conceptual or doctrinal framework, normative legal research is also referred to as rule-based or dogmatic research, and essentially involves the inventory and analysis of positive law while containing a prescriptive dimension (Marzuki, 2005). In line with this framework, to examine the issues addressed in this study in greater depth, the researcher presents relevant findings derived from primary legal materials originating from statutory regulations as well as secondary legal materials obtained from scientific literature. The research approaches employed in this study are the statutory approach and the conceptual approach (Kristiawanto, 2022).



3. RESULTS AND DISCUSSION

The Development of Digital Technology as a Factor in the Emergence and Growth of Cybercrime: Reflections on the Ethical Crisis in the Digital Age

Contemporary digital civilization is confronting one of its greatest paradoxes. As human existence increasingly migrates from the constraints of the physical world to the boundless realm of cyberspace, the moral foundations that once governed human behavior are experiencing an existential fracture. The growing prevalence of cybercrime should therefore not be understood merely as a failure of computer security systems; rather, it represents a tangible manifestation of the erosion of human ethical values when individuals act anonymously behind digital interfaces, detached from physical presence and direct social accountability.

The advancement of digital technology constitutes one of the most remarkable achievements in the history of human civilization. Digitalization has transformed nearly every aspect of modern life, including communication, economic activities, education, healthcare, and systems of governance. The emergence of the Internet, Artificial Intelligence (AI), cloud computing, the Internet of Things (IoT), blockchain technology, and big data analytics has dramatically accelerated the exchange of information beyond the limitations of time and geographical boundaries. Nevertheless, beneath these unprecedented technological achievements lies a profound paradox. As technological innovation continues to advance, the threats confronting humanity become increasingly sophisticated and multidimensional. Within this context, cybercrime should not be viewed solely as an inevitable consequence of technological progress but rather as a reflection of the ethical crisis accompanying contemporary digital transformation.

From a philosophical perspective, technology is inherently value-neutral. Technology itself neither determines whether a particular action is morally right nor morally wrong; instead, moral significance is assigned by those who employ it. Without a solid ethical foundation, technological advancement inevitably gives rise to a paradox of civilization: the more sophisticated human technology becomes, the more fragile the moral values sustaining that civilization may become. When moral development fails to keep pace with rapid digital innovation, technology gradually loses its humanistic orientation and is transformed into an instrument of exploitation, manipulation, and even the degradation of human dignity.

The postmodern philosopher Jean Baudrillard introduced the concept of simulacra, describing a condition in which digital images and representations replace authentic reality to such an extent that the distinction between the real and the simulated becomes virtually indistinguishable—a phenomenon he referred to as hyperreality (Baudrillard, 1994). Within



cyberspace, money is reduced to numerical values displayed on digital screens, personal identity is reconstructed as an avatar, and the suffering of victims is often diminished to nothing more than a sequence of textual complaint reports. Such a transformation fundamentally alters human perceptions of reality and ethical responsibility.

When reality is obscured by simulation, traditional moral understandings of concepts such as “sin” and “crime” gradually lose their normative significance. Individuals engaged in cybercrime, including operators of illegal online gambling platforms, perpetrators of disinformation campaigns that destroy personal reputations, or credit card hackers, often do not perceive themselves as committing serious moral wrongdoing. Instead, they become immersed in the hyperreality of digital interaction, where stealing digital assets may appear no more consequential than achieving victory in a video game.

A similar phenomenon emerges when algorithmic systems subordinate moral considerations to economic incentives, giving rise to what scholars describe as moral disengagement. Digital platforms frequently allow hatred, deception, and social polarization to proliferate because such content generates substantial user engagement and commercial value. Cybercrime flourishes within this structural environment. Rather than technology being governed by human ethical principles, the most destructive human impulses—including greed, hostility, and manipulation—are amplified by the architecture of digital technologies themselves. Consequently, modern individuals gradually lose their moral agency and become increasingly subordinated to digitally mediated desires (Borgmann, 1984).

These developments reveal a widening disparity between technological capability and moral capability. Digital civilization has progressed at a pace far exceeding humanity's capacity to cultivate ethical responsibility. As a consequence, digital space has evolved beyond its original function as a medium of communication and innovation into a new arena for diverse forms of social deviance. Contemporary cybercrime encompasses identity theft, online fraud, ransomware attacks, unauthorized system intrusions, malware distribution, illicit trafficking of personal data, online child sexual exploitation, and information manipulation through Artificial Intelligence technologies such as deepfakes. Recognizing the transnational nature of these emerging threats, the United Nations Convention against Cybercrime emphasizes that advances in information technology have created new forms of cross-border criminality requiring extensive international cooperation, as perpetrators are able to operate across jurisdictions while exploiting the anonymity afforded by cyberspace (United Nations Digital Library, 2024).



From the perspective of moral philosophy, this condition reflects what Hans Jonas (1984) describes as the principle of responsibility. Jonas argues that the greater humanity's power becomes through technological advancement, the greater the moral responsibility that must accompany it. Accordingly, the fundamental challenge confronting contemporary digital society is not the absence of innovation but rather the insufficiency of ethical responsibility in its application. Technology provides individuals with unprecedented capacities to influence the lives of others; however, it does not inherently cultivate the wisdom required to exercise such power responsibly. Consequently, cybercrime should be understood as a manifestation of the misuse of human freedom when technological capabilities are not balanced by corresponding ethical responsibility (Jonas, 1984).

A comparable perspective is advanced by Luciano Floridi through his theory of Information Ethics. Floridi argues that digital transformation has given rise to a new environment known as the infosphere, a dynamic informational ecosystem in which human beings, data, computer systems, and artificial intelligence continuously interact. Within this ecosystem, every action involving information carries moral implications. Acts such as stealing personal data, manipulating digital identities, or disseminating false information inflict harm not only upon technological systems but also upon the integrity of human beings as integral participants in the informational ecosystem. From this perspective, cybercrime extends beyond the scope of legal transgression and constitutes an act that undermines the moral equilibrium of the digital environment.

The ethical philosophy of Immanuel Kant likewise provides a compelling normative foundation for understanding cybercrime. Kant maintains that every human being must always be treated as an end in itself, rather than merely as a means to achieve another's objectives. In many forms of cybercrime, however, victims are reduced to economic objects or instruments of exploitation. Personal data are commodified, digital identities are falsified, and individual privacy is violated for financial gain. Such practices directly contradict the Kantian principle of respect for human dignity because they transform individuals into mere instruments for advancing the interests of perpetrators (Kant, 1998).

Furthermore, the rapid development of digital technology exemplifies what Zygmunt Bauman conceptualizes as liquid modernity, a social condition in which norms and values become increasingly fluid in response to continuous and accelerated change. Within digital society, interpersonal relationships are progressively mediated by technology, while traditional mechanisms of social control gradually weaken. The anonymity afforded by the Internet



diminishes individuals' sense of accountability for the consequences of their actions. As a result, acts such as online fraud, hate speech, data theft, and cyberattacks can be committed without direct confrontation between offenders and victims. The disappearance of face-to-face interaction consequently reduces empathy, making harmful behavior toward others easier to rationalize and perpetrate.

The emergence of Artificial Intelligence (AI) has further intensified this ethical dilemma. AI technologies are now capable of generating text, images, voices, and videos that are increasingly indistinguishable from authentic reality. On the one hand, these innovations significantly enhance efficiency and productivity across numerous sectors. On the other hand, the same technologies facilitate the creation of deepfakes, automated phishing schemes, digital identity manipulation, and increasingly sophisticated cyberattacks. These developments illustrate the inherently ambivalent nature of technological progress. While technology creates unprecedented opportunities for human advancement, it simultaneously amplifies the potential for abuse when not guided by adequate ethical oversight.

From a sociological perspective, the expansion of the digital economy has also generated substantial incentives for cybercriminal activities. The economic value of personal data continues to increase, transforming information into one of the most valuable commodities of the digital era. Personal identities, banking credentials, consumer behavior, and individual preferences possess significant commercial value within illicit digital marketplaces, commonly referred to as the dark web. Consequently, financial motivation has become one of the principal drivers behind the growing frequency of cyberattacks targeting individuals, private enterprises, and public institutions alike. International reports further indicate that advances in information technology have fundamentally transformed the structure of organized crime by expanding transnational criminal networks, lowering barriers to entry for offenders, and increasing the operational efficiency of digitally enabled criminal enterprises (Nations, 2026).

These developments demonstrate that the fundamental cause of cybercrime does not lie in technology itself but rather in the crisis of values within contemporary digital society. Erich Fromm distinguishes two fundamental orientations of human existence: the mode of having and the mode of being. In modern digital culture, the orientation toward having increasingly dominates human life. Success is frequently measured by the accumulation of economic wealth, social media popularity, and control over information. When such an orientation evolves without the restraint of moral values, technology is transformed into an instrument for pursuing personal gain by any available means, including criminal conduct.



Accordingly, the advancement of digital technology should be understood as a phenomenon encompassing two inseparable dimensions. The first is the technological dimension, which drives innovation and the progress of civilization. The second is the moral dimension, which determines the ethical direction in which technology is developed and utilized. Cybercrime emerges when technological development progresses more rapidly than ethical development. Therefore, addressing cybercrime cannot rely solely on strengthening digital security infrastructures or enhancing legal enforcement. It must also involve the cultivation of digital ethics that places human beings at the center of technological advancement. A sustainable digital civilization can be achieved only when technological progress advances in harmony with the reinforcement of honesty, responsibility, justice, respect for privacy, and the protection of human dignity. Without such an ethical foundation, technological advancement inevitably produces a paradox of civilization: the more sophisticated human technology becomes, the more fragile the moral values sustaining that civilization become.

The most sophisticated forms of contemporary cybercrime no longer primarily target computer infrastructure; instead, they target human cognition, a phenomenon increasingly described as cognitive hacking. When truth itself can be manufactured, manipulated, and disseminated on a massive scale to advance political or economic interests, the moral foundations of society begin to erode. In the absence of a shared and universally accepted understanding of what is true and false, structured disinformation is no longer widely perceived as a criminal act but rather as a strategic instrument or merely another tactic of asymmetric warfare.

Consequently, combating cybercrime will never be achieved solely by upgrading firewalls or enacting new criminal legislation. What is fundamentally required is the reconstruction of digital ethics (Techno-Ethics), a normative framework that reminds humanity that behind every pixel on a digital screen lies another human being whose inherent dignity and fundamental rights deserve unwavering respect. Only by integrating technological innovation with ethical responsibility can digital civilization continue to evolve in a manner that is secure, humane, and sustainable.

Efforts to Combat Cybercrime Through The Enforcement of Laws, The Promotion of Digital Ethics, and The Improvement of Digital Literacy to Create a Safe and Responsible Cyberspace

Confronting the growing wave of cybercrime in the digital era requires far more than strengthening technological defenses alone; it demands the restoration of the moral foundations of civilization itself. As virtual space increasingly transforms into an anarchic digital frontier, efforts

to combat cybercrime must be reoriented toward their fundamental humanistic purpose through a triadic approach that integrates the authority of law as the guardian of external conduct, the guidance of ethics as the compass of moral conscience, and the empowerment of digital literacy as the foundation of critical and responsible reasoning.

Cyber law, including Indonesia's Electronic Information and Transactions Law (EIT Law), the Personal Data Protection Law (PDP Law), and the General Data Protection Regulation (GDPR) of the European Union, should not be regarded merely as a punitive instrument. Rather, it establishes the ontological boundaries of digital existence by affirming that actions performed in cyberspace produce tangible consequences in the physical world. In this sense, the law restores the sense of embodiment and accountability that is often obscured by digital anonymity, reminding individuals that freedom in virtual environments is inseparable from responsibility and must always be exercised with due regard for the fundamental rights of others.

Law has historically emerged as an instrument for establishing social order, ensuring justice, and protecting fundamental human rights. Aristotle argued that the ultimate purpose of law is the realization of justice, which constitutes the foundation of communal life. Within the context of digital society, law serves to maintain a balance between individuals' freedom to utilize technological innovation and their responsibility to ensure that such freedom does not infringe upon the rights and interests of others. Without an effective legal framework, cyberspace risks evolving into an unregulated domain dominated by power, competing interests, and exploitation. Accordingly, the enforcement of cyber law is intended not only to punish offenders but also to restore public confidence in justice and strengthen trust within the digital ecosystem.

Nevertheless, the legal philosopher Gustav Radbruch emphasized that law must not be guided solely by legal certainty, but must also uphold the principles of justice and expediency. This perspective is particularly relevant in addressing the rapidly evolving nature of cybercrime, where technological innovation continually generates new forms of criminal activity. Legal frameworks that remain rigid and static inevitably lag behind the evolving methods employed by cybercriminals. Consequently, legal systems must be adaptive, responsive, and capable of anticipating emerging technologies, including Artificial Intelligence, cloud computing, the Internet of Things (IoT), and blockchain technology. In this regard, the United Nations Convention against Cybercrime underscores the importance of harmonizing national legal systems, strengthening international cooperation, facilitating the exchange of electronic evidence, and enhancing the institutional capacity of law enforcement agencies to address the transnational character of cybercrime (Radbruch, 2006).



Despite its indispensable role, law possesses inherent limitations. Legal mechanisms generally operate only after a violation has occurred, whereas ethics functions preventively by guiding individuals before unlawful conduct takes place. Ethics represents the voice of conscience that enables individuals to distinguish right from wrong even in the absence of external supervision or state coercion. Immanuel Kant maintained that genuinely moral conduct does not arise from fear of punishment but from an individual's recognition of moral duty toward others. Accordingly, the effective prevention of cybercrime cannot depend solely on the deterrent effect of criminal sanctions. Rather, it requires the internalization of ethical values within every individual who participates in the digital environment, ensuring that technological freedom is consistently exercised with integrity, responsibility, and respect for human dignity.

This necessity has given rise to the concept of digital ethics, defined as a set of normative principles governing the responsible use of digital technologies. Digital ethics emphasizes that every activity conducted in cyberspace should respect the right to privacy, safeguard information security, prevent the dissemination of disinformation, uphold intellectual property rights, and preserve human dignity. Through his theory of Information Ethics, Luciano Floridi argues that information should not be regarded merely as an object of exchange but rather as an integral component of the moral ecosystem known as the infosphere. Consequently, acts such as data destruction, digital identity theft, malware dissemination, and information manipulation constitute not only legal violations but also forms of moral harm that disrupt the ethical equilibrium of the informational ecosystem (Floridi, 2013).

The importance of digital ethics is further reinforced by Hans Jonas's *The Imperative of Responsibility*. Jonas contends that technological advancement continually expands humanity's capacity to influence the lives of others. Accordingly, every increase in technological power must be accompanied by a corresponding increase in moral responsibility. Within contemporary digital society, a single social media post, algorithm, or artificial intelligence system can influence millions of individuals simultaneously. Such conditions demand the development of ethical awareness that recognizes every digital action as carrying broad social consequences. Digital ethics, therefore, should not be understood merely as a code of conduct but as the moral foundation that ensures technological progress remains aligned with fundamental human values (Jonas, 1984).

Alongside the strengthening of legal frameworks and ethical principles, digital literacy constitutes the third essential pillar in the effective prevention of cybercrime. Digital literacy extends far beyond the technical ability to operate digital devices. It encompasses critical thinking, the capacity to evaluate information, an understanding of digital risks, the ability to protect

personal data, and the competence to make ethically informed decisions within digital environments. UNESCO emphasizes that Digital Citizenship Education should integrate knowledge, practical skills, ethical values, attitudes, and civic responsibility to enable individuals to participate safely, responsibly, and constructively in digital society (UNESCO, 2024).

Digital literacy may also be understood as a process of cultivating practical wisdom (phronesis), as conceptualized by Aristotle. Technical competence without wisdom merely produces individuals who are capable of using technology but not necessarily capable of using it responsibly. By contrast, digital literacy grounded in practical wisdom fosters individuals who are not only technologically proficient but also ethically mature. From this perspective, digital education should extend beyond teaching technical Internet skills to nurturing moral character and self-discipline amid the overwhelming flow of digital information.

The importance of digital literacy has become even more apparent with the increasing complexity of threats driven by artificial intelligence. Technologies such as deepfakes, generative artificial intelligence, social engineering, and automated phishing have become progressively more sophisticated and difficult for ordinary users to identify. Consequently, efforts to strengthen digital literacy must be pursued continuously through formal education, community training programs, public awareness campaigns, and lifelong learning initiatives. UNESCO further emphasizes that digital citizenship should be developed through an integrated approach combining media literacy, ethical education, critical thinking, and social responsibility, thereby equipping society to respond more wisely to the challenges posed by the age of artificial intelligence (UNESCO, 2024).

Ultimately, combating cybercrime requires a framework of collaborative governance. The security of cyberspace cannot be regarded solely as the responsibility of governments or law enforcement agencies; rather, it demands the collective engagement of the state, the private sector, educational institutions, technology communities, civil society organizations, and every individual Internet user. This collaborative approach is consistent with Jürgen Habermas's theory of communicative action, which maintains that social order can only be sustained through dialogue, participation, and shared responsibility. Within the digital environment, such collaboration may be realized through the development of robust cybersecurity standards, the strengthening of personal data protection, the enhancement of law enforcement capacity, the establishment of effective cyber incident reporting mechanisms, and the promotion of public education on digital security.

A secure cyberspace should ultimately be understood as the manifestation of the classical concept of *bonum commune*, or the common good. Thomas Aquinas maintained that the fundamental purpose of law and social governance is to promote the common good rather than

merely safeguarding the interests of particular individuals. This principle remains highly relevant to the governance of contemporary digital society. Cybersecurity should therefore not be viewed solely as the protection of computer systems and digital infrastructures, but as the protection of fundamental human rights, social trust, economic stability, and the sustainability of democratic institutions. When individuals feel secure in their use of digital technologies, cyberspace can flourish as an environment that fosters innovation, creativity, and the continued advancement of human civilization (Aquinas, 1946).

Accordingly, combating cybercrime requires a holistic and integrated approach. The effective enforcement of law provides legal certainty while safeguarding the rights and interests of society. The promotion of digital ethics cultivates the moral awareness necessary for individuals to employ technology responsibly and with respect for others. Meanwhile, strengthening digital literacy equips society with the critical thinking skills and resilience needed to confront the increasingly complex challenges of the digital environment. These three pillars are mutually reinforcing and cannot function effectively in isolation. Law without ethics produces compliance motivated merely by fear of sanctions. Ethics without digital literacy remains an aspirational ideal that is difficult to translate into responsible digital behavior. Digital literacy without the support of law lacks the institutional authority necessary to deter and address violations effectively. Consequently, a secure, responsible, and sustainable cyberspace can only be realized when law, digital ethics, and digital literacy evolve in a balanced and complementary manner, serving as the fundamental pillars of a digital civilization founded upon justice, civility, and unwavering respect for human dignity.

4. CONCLUSIONS

The advancement of digital technology has ushered human civilization into a new era characterized by rapid progress in communication, economic activities, education, governance, and numerous other aspects of human life. Despite these significant benefits, digital transformation has also given rise to a paradox of civilization. The rapid pace of technological advancement has not always been accompanied by a corresponding development of human moral consciousness. Consequently, cyberspace has evolved not only as a platform for innovation and information exchange but also as an environment in which various forms of cybercrime, including data theft, online fraud, system hacking, ransomware attacks, the dissemination of disinformation, and the misuse of artificial intelligence, have increasingly emerged. This phenomenon demonstrates that the root cause of cybercrime does not lie in technology itself but rather in the ethical crisis



confronting digital civilization, as reflected in the erosion of moral responsibility, respect for human dignity, and awareness of the social consequences of actions performed in digital environments. Accordingly, cybercrime should be understood as a manifestation of the imbalance between technological advancement and the development of fundamental human values.

The prevention and mitigation of cybercrime cannot rely solely on a repressive approach through law enforcement, as the evolution of digital crime consistently outpaces the capacity of legal and regulatory frameworks to respond effectively. Accordingly, a holistic and sustainable strategy is required, integrating adaptive legal enforcement, the promotion of digital ethics, and the enhancement of public digital literacy. Law provides legal certainty and safeguards the rights and interests of society; digital ethics fosters the moral awareness necessary for the responsible use of technology; while digital literacy equips individuals with the critical thinking skills needed to understand digital risks, protect information security, and navigate the digital environment responsibly. These three pillars must be reinforced through collaborative efforts involving governments, law enforcement agencies, educational institutions, the private sector, digital communities, and society at large as a shared responsibility for safeguarding cyberspace. Ultimately, a secure, just, and responsible digital environment can only be realized when technological advancement is consistently guided by the principles of justice, accountability, respect for human rights, and ethical wisdom. In this way, technology serves not merely as an instrument of progress but also as a means of strengthening a civilized human society founded upon the pursuit of the common good.

REFERENCES

- Soekanto, S. &. (2010). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: RajaGrafindo Persada.
- Social, W. a. (2025, Februari 5). *Digital 2025: The essential guide to the global state of digital* . Jakarta: PT We are Social Indonesia. Dipetik 2025, dari We are Social: <https://wearesocial.com/id/blog/2025/02/digital-2025-the-essential-guide-to-the-global-state-of-digital/>
- APJII. (2024, Februari 7). *Asosiasi Penyelenggara Jasa Internet Indonesia*. Diambil kembali dari <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>
- Yarbrough, C. (2024, Desember 3). *Internet Crime Complaint Center (IC3)*. Dipetik Desember 2024, dari IC3 Annual Report: https://www.ic3.gov/AnnualReport/Reports/2024_ic3report.pdf



- Heidegger, M. (1977). *The Question Corcening Technologi and Other Essay*. New York, London: Garland Publishing, INC.
- Baudrillard, J. (1994). *Simulacra and Simulation Translated* . The United States of America : The University of Michigan Press.
- Borgmann, A. (1984). *Technologi and the Character of Contemporary Life A Philosophical Inquiry*. London: The University of Chicago Press.
- Nations, U. (2026, Maret 26). *United Nations Office on Drugs and Crime*. Diambil kembali dari https://www.unodc.org/roseap/uploads/documents/Publications/2025/2025.10.21_The_Nexus_Between_Cybercrime_and_Corruption.pdf?utm_source=chatgpt.com
- Nations, U. (2024, Maret). Diambil kembali dari United Nations Digital Library: <https://digitallibrary.un.org/search?f1=author&as=1&sf=title&so=a&rm=&m1=e&p1=UN.+General+Assembly+%2879th+sess.+%3A+2024-2025%29&ln=en>
- Hans, J. (1984). *The Imperative of Responsibility In Search of an Ethics for the Technological Age*. London: The University of Chicago Press.
- Kant, I. (1998). *Groundwork of the Metaphysics of Morals*. Cambridge: Cambridge University Press.
- Unesco. (2024, Maret 14). Diambil kembali dari Unesco: https://www.unesco.org/en/articles/qa-why-digital-global-citizenship-education-essential?utm_source=chatgpt.com
- Aquinas, T. (1946). *Summa Theologica*. Oxford: Christian Classic Ethereal Library.
- Radbruch, G. (2006)). *Statutory Lawlessness and Supra-Statutory Law* . Oxford: Oxford Journal of Legal Studies.
- Floridi, L. (2013). *The Ethics of Information*. Oxford: Oxford University Press.
- Jonas, H. (1984). *The Imperative of Responsibility*. London: The University of Chicago Press .
- Kristiawanto, S. H. I. (2022). *Memahami Penelitian Hukum Normatif*. Prenada Media.
- Marzuki, P. M. (2005). *Penelitian hukum*.

