BIS HUMANITIES AND SOCIAL SCIENCE

Volume 4 2026 | DOI: 10.31603/bishss.433
7th Borobudur International Symposium on Humanities and Social Science (BIS-HSS) 2025

UNIMMA PRESS
Universitas Muhammadiyah Magelang

# From algorithms to crime: A criminal law analysis of the use of bots to manipulate public opinion

Ni Putu Rai Yuliartini[1*], Dewa Gede Sudika Mangku[1], and Gede Sariasa[1]

[1] Universitas Pendidikan Ganesha, Buleleng, Indonesia
[*]Corresponding author's email: raiyuliartini@undiksha.ac.id

## Abstract

The development of information and communication technology has brought about various innovations in the digital space, including the use of bots, or automated programs, on the internet. However, the emergence of bots does not always have a positive impact. The phenomenon of the massive use of bots to manipulate data and shape public opinion on social media has become a serious issue in the context of criminal law. This study aims to analyze criminal liability for the use of bots for manipulative purposes and examine the relevance of national criminal law provisions in addressing this practice. The research method used is a normative juridical approach, by examining applicable laws and regulations, legal literature, and relevant cases. The analysis shows that the use of bots to spread false information, conduct cyberattacks, or manipulate public opinion can be classified as a criminal offense under the provisions of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), as amended by Law Number 19 of 2016, and can be linked to the Criminal Code (KUHP), specifically regarding the crimes of fraud, slander, and unlawful acts that harm others. Furthermore, the lack of specific regulations regarding bots in Indonesian positive law presents unique challenges for law enforcement. Therefore, strengthening criminal law regulations and policies that explicitly govern the use of automated systems in cyberspace is necessary to ensure protection of data integrity, healthy freedom of expression, and fairness in the digital ecosystem.

**Published:**
May 04, 2026



Selection and Peer-review under the responsibility of the 7th BIS-HSS 2025 Committee

## Keywords

Criminal law, internet bots, data manipulation, public opinion, ITE law

## Introduction

In the last decade, advances in digital technology based on algorithms and artificial intelligence (AI) have brought fundamental changes to the social, economic, and political lives of global society [1]. This technology has not only changed the way humans communicate and interact, but has also reshaped the structure of information power, where algorithms now play a major role in determining what the public sees, reads, and believes. One concrete manifestation of this development is the emergence of bots,

namely automated programs designed to perform specific tasks in cyberspace without direct human involvement [2]. Bots can operate on a massive scale, working 24/7, and are able to replicate human behavior in digital activities such as liking, sharing, or commenting on content on social media.

The phenomenon of bot use, initially developed for productive purposes such as providing automated customer service, accelerating information searches, or supporting e-commerce activities, has now given rise to new dimensions of social and legal issues [3]. In recent years, bots have been widely used to spread political messages, reinforce certain narratives, and create the impression of public support for certain issues through algorithmic manipulation techniques. This practice is known as "computational propaganda", which is the use of automated systems and digital data to influence public opinion and political behavior [4]. As a result, the digital public space, which should be an arena for open and participatory dialogue, has become vulnerable to information manipulation and perception manipulation.

From a criminal law perspective, this phenomenon is a serious issue because it involves the use of technology for manipulative purposes that can mislead the public and disrupt public order. Bots driven by certain algorithms can be used to systematically spread fake news, hate speech, and disinformation, thereby affecting social stability and even democratic processes [5]. In the context of elections, for example, political bots are able to massively duplicate messages to support a particular candidate or undermine their opponent, creating the illusion of public opinion that appears natural, when in fact it is the result of algorithmic engineering. This phenomenon has occurred in various countries, including the United States, Russia, and several Eastern European countries, where bots are used as a tool of modern political propaganda [6].

In Indonesia, the use of bots to manipulate public opinion has become a serious concern, particularly since the increased use of social media in political campaigns and the dissemination of public issues. Several reports indicate that thousands of automated accounts are being used to spread hoaxes, reinforce social polarization, or shape certain public sentiments [7]. This raises concerns about the public's vulnerability to digital manipulation and highlights legal gaps in regulating and enforcing criminal liability for the perpetrators behind these automated systems. Although the Electronic Information and Transactions Law (UU ITE) prohibit the dissemination of false information and hate speech, this law does not specifically address the use of algorithms or bots as a means of digital crime.

This issue is crucial because bots are no longer merely neutral technological tools, but have become instruments capable of manipulating public opinion, distorting the flow of information, and, in some cases, threatening the integrity of democracy and social order. Therefore, a key issue that needs to be examined is how criminal law can address the use of algorithmic technologies like bots when they are exploited for manipulative purposes that harm society and the state.

Various previous studies have shown that the use of social media and algorithmic technology, particularly bots, has posed serious challenges to the legal system and public information governance in the digital era. A study by Devi Rahma Fatmala, Amanda Amelia, and Fitri Agustina Trianingsih (2020), entitled " *The Use of Social Media Bot Accounts on Influencing Public Opinion: A Legal Review in Indonesia* ," explains that bot accounts are automated, algorithm-based programs designed to carry out activities on social media without direct human involvement. Through a normative and conceptual legal approach, the study highlights how bots are used to amplify political messages, replicate certain narratives, and influence public opinion on a large scale. This practice is known as computational propaganda, where algorithms are used to shape public perception and shift public opinion according to the interests of certain parties. The study emphasizes that this phenomenon has the potential to undermine the principles of deliberative democracy by creating social polarization, disinformation, and inequality in the public discourse space. From a legal perspective, Fatmala and colleagues found that Indonesia does not yet have regulations specifically governing the use of bot accounts for political or economic interests. The provisions of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) only address the dissemination of false or misleading information, without addressing the mechanisms for using automated algorithms as tools for information manipulation. Therefore, this study recommends the need for regulatory updates that emphasize transparency, accountability, and legal responsibility for those who create and control bots in the digital space [8].

Meanwhile, research conducted by Fransiskus Nomor, Ida Bagus Anggapurana Pidada, and Kadek Fredi Andrika Adnantara (2024) in the Jembatan Hukum journal entitled "Law Enforcement against Social Media Misuse in Building Public Opinion in the 2024 Election" provides a more applicable perspective on the practice of social media misuse in the Indonesian political context. Using normative juridical methods and a legislative approach, this study examines how social media has become an important instrument in shaping public opinion during the election process, as well as a potential means for political manipulation. The authors identify forms of social media misuse such as the spread of hoaxes, smear campaigns, hate speech, and the use of fake accounts or bots to build a certain political image. The findings of this study indicate that although the ITE Law and Law Number 7 of 2017 concerning General Elections contain provisions regarding the prohibition of the dissemination of false information and hate speech, their enforcement is still weak and unable to reach new patterns of crime committed through algorithmic systems. The author also emphasizes that law enforcement officers still face obstacles in proving cases involving automated digital activity, both due to limited legal instruments and low technical capacity and legal awareness among officers. Therefore, this study recommends the need to improve the professionalism of law enforcement officers, provide digital education for the public, and establish stricter regulations regarding the use of social media for political purposes to prevent distortions of the principles of justice and democratic integrity [9].

In general, both studies share a common thread: highlighting legal vulnerabilities in addressing the misuse of digital technology in shaping public opinion. Fatmala et al.'s research focuses more on the theoretical and normative aspects regarding the need for specific regulations regarding the use of bot accounts in the context of digital democracy, while Fransiskus Nomor et al.'s research focuses on the practical aspects of law enforcement in the field, particularly during elections. Both agree that Indonesian positive law does not yet have adequate tools to address the phenomenon of algorithmic manipulation on social media. This regulatory gap opens up space for digital propaganda practices that can undermine the democratic order and public trust in information. Therefore, the results of these two studies provide an important foundation for further research focused on strengthening the criminal law framework in addressing algorithmic crimes, including the use of bots to manipulate public opinion. By strengthening substantive legal aspects and technology-based law enforcement, it is hoped that Indonesia can build a legal system that is more responsive to the challenges of the era of algorithms and artificial intelligence, so that the digital space remains a healthy, transparent, and democratic platform.

This gap in criminal law studies demonstrates that while the social impacts of bot use have been extensively researched, the legal accountability for the use of algorithms for manipulative purposes still lacks a clear analytical framework. In the Indonesian legal context, this phenomenon is further complicated by the lack of criminal law regulations explicitly governing the use of bots to influence public opinion. Existing regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, only prohibit the dissemination of false information, insults, or hate speech, without addressing the mechanisms of using automated algorithms to disseminate such information [10]. Consequently, the systematic misuse of bot technology for political or economic purposes is difficult to qualify as a criminal offense. This is where a normative gap emerges that needs to be explained conceptually and legally through criminal law studies.

In a comparative context, several countries have developed legal frameworks that are more adaptive to algorithmic challenges. For example, the European Union, through its Digital *Services Act* (2022) and *AI Act* (2023), introduced the principles of *algorithmic accountability* and *transparency obligation* , which require that every algorithmic system be audited and held legally accountable [11]. In the United States, the concept of *algorithmic responsibility* has begun to be introduced in the context of the spread of political disinformation and digital market manipulation. These studies indicate that legal systems in various jurisdictions are shifting from a passive approach to an active regulatory paradigm regarding algorithms and bots [12]. However, at the global level, discourse on the application of criminal law to acts of digital manipulation is still minimal, and in Indonesia, there is almost no in-depth research discussing it from a dogmatic perspective of criminal law.

Considering this gap, this study offers a conceptual approach to link the use of bots as means *and* algorithms as causal *elements* in the crime of public opinion manipulation. This approach positions algorithms not merely as technical tools, but as part of the actus reus ( *actus reus* ) that can have legal consequences if used for purposes that violate the public interest. Thus, this study seeks to develop a new framework for how criminal law can be applied to assess the responsibility of perpetrators in the digital era, where some acts are carried out by automated systems that operate without human awareness. This approach departs from the theories of *strict liability* and *vicarious liability* in modern criminal law, which can be used to assess the responsibility of corporations, creators, or bot users in cases of digital manipulation [13].

Furthermore, this research also seeks to provide a theoretical contribution to the development of cybercriminal law *by* expanding the scope of technology-based crimes beyond conventional crimes such as hacking and data theft to new forms of behavioral *and* algorithmic *crimes.* The phenomenon of manipulating public opinion with bots demonstrates that crimes in the digital world do not always take the form of attacks on systems, but can also be attacks on the collective consciousness of society through the systematic dissemination of misleading information. Therefore, criminal law needs to emphasize its role not only as a means of punishment, but also as an instrument for protecting the public interest against algorithmic threats that have the potential to disrupt social stability and democracy.

From a methodological perspective, this research employs a normative legal approach with two primary analytical tools: a statutory approach *and* a conceptual approach. The statutory approach is used to examine relevant positive legal norms, including the Electronic Information and Transactions Law (ITE Law), the Criminal Code (KUHP), and various regulations related to cybersecurity, as well as international legal instruments such as the Budapest Convention on Cybercrime (2001) and the OECD Guidelines on AI Governance (2022). The conceptual approach, meanwhile, is used to build a theoretical foundation regarding the relationship between algorithms, criminal liability, and the protection of the public interest.

Overall, this study aims to provide a criminal law analysis of the use of bots in manipulating public opinion, emphasizing the importance of reformulating criminal norms relevant to the dynamics of modern technology. Through this research, it is hoped that a normative framework can be found that bridges the gap between algorithmic advancements and the need for legal certainty, while simultaneously strengthening the position of criminal law as a tool to maintain the integrity of the digital public sphere. Thus, this study not only contributes to the development of cybercriminal law theory but also provides direction for policymakers in designing regulations that are more responsive to the ethical, social, and legal challenges of the algorithmic era.

## Method

The research method used in this study is normative legal research or doctrinal legal research. This research focuses on the study of positive legal norms, legal principles, and relevant legal doctrines to answer the question of how criminal law can be applied to the use of algorithms and bots in manipulating public opinion in the digital space [14]. Through a literature review, this research examines applicable legal regulations and criminal law concepts that can be used to explain legal responsibility in the context of autonomous technology.

This research uses two main approaches: the statutory approach *and the* conceptual approach. The statutory approach is used to examine various national and international legal provisions related to cybercrime and technology abuse, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 1 of 2023 concerning the Criminal Code (New Criminal Code), and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) [15]. At the international level, key references include the Budapest Convention on Cybercrime (2001) and the European Union's Digital Services Act (2022). This approach aims to assess the extent to which existing legal frameworks are able to accommodate new forms of algorithm-based digital crime.

Meanwhile, a conceptual approach is used to develop a theoretical framework regarding the relationship between algorithms, bots, and criminal liability [16]. This approach examines concepts such as strict liability, vicarious liability, and corporate criminal responsibility to explain the potential expansion of legal subjects in the context of digital crimes, some of which are carried out by automated systems.

The legal materials used consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation and international legal instruments; secondary legal materials include academic literature, scientific articles, and previous research results; while tertiary legal materials include legal dictionaries and legal encyclopedias [17]. The analysis of legal materials is conducted qualitatively through the classification, interpretation, and evaluation of legal norms with grammatical, systematic, and teleological interpretations [18].

Using a normative legal research method that combines statutory and conceptual approaches, this research is expected to provide a comprehensive understanding of the role of criminal law in regulating and enforcing legal responsibility for the use of algorithms and bots in manipulating public opinion [19]. Furthermore, the results of this research are expected to contribute to the development of modern criminal law doctrine that is more adaptive to technological advances, while strengthening the protection of the public interest, privacy rights, and democratic integrity in the increasingly complex era of digital communication.

## Results and Discussion

### *Results*

The research findings show that the phenomenon of using algorithms and bots to manipulate public opinion has become one of the most crucial issues in modern criminal law studies. In the context of an increasingly automated digital world, the use of algorithm-based systems and artificial intelligence (AI) not only influences the way humans communicate and interact, but also shapes the way people think, express opinions, and make social and political choices [20]. Automated bot programs controlled by specific algorithms can work massively to spread messages, duplicate narratives, and shape public opinion at a speed and reach far beyond human capabilities. This phenomenon raises serious concerns because bots no longer function merely as technological aids but have also been used as instruments of social and political manipulation capable of changing public perception and threatening the integrity of democracy [21]. From a criminal law perspective, this condition creates new issues regarding the limits of responsibility and legal regulation of non-human entities capable of causing significant legal consequences for society.

Through a review of national laws and international legal instruments, it was found that the legal framework in Indonesia does not explicitly regulate criminal liability for the use of automated or algorithmic systems exploited for manipulative purposes in the digital space [22]. Current regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendment in Law Number 19 of 2016, do prohibit the dissemination of false information, hate speech, and content detrimental to the public interest. However, these norms are still oriented towards direct human actions and do not yet cover the use of algorithms, bots, or artificial intelligence systems as a means of committing crimes. This means that when unlawful acts are committed by automated systems operating based on specific commands or patterns, the law still has difficulty determining who can be held criminally responsible.

In this context, the New Criminal Code (Law Number 1 of 2023) has also not shown significant progress. Classical principles in criminal law that rely on the elements of fault (*schuld*) and moral awareness (*mens rea*) are not easily applied to systems that operate automatically. For example, if an algorithm is set to amplify a particular message or increase the number of posts of misleading political opinions without direct human involvement, it is legally difficult to prove who the perpetrator had malicious intent (*intent*). Whether the algorithm code creator, the bot user, or the party who ordered and profited from the dissemination of the information should be held criminally responsible remains a conceptual issue that has not been clearly regulated in national law.

Furthermore, Indonesian regulations do not yet recognize algorithmic criminal accountability mechanisms, as implemented in several international jurisdictions. Globally, the European Union has been a pioneer in addressing the relationship between

technology and law through regulations such as the Digital Services Act (2022) and the AI Act (2023). Both regulations emphasize the principle of *algorithmic accountability.* (algorithmic accountability) and *transparency obligation,* which require that any algorithmic system with the potential to influence the public sphere be regularly audited, have clear controls, and be legally accountable. Similarly, the Budapest Convention on Cybercrime (2001) introduced international standards for regulating crimes involving digital technology, including crimes committed through automated systems. Unfortunately, Indonesia has yet to adopt similar regulations, despite the increasing vulnerability of society to the misuse of algorithms and bots.

This lack of clear regulations creates a legal gap *that* has the potential to hinder law enforcement against perpetrators of digital crime. As a result, phenomena such as the spread of disinformation, covert political campaigns, and the manipulation of public opinion on social media cannot be effectively prosecuted under criminal laws. In practice, the law only applies to individuals or groups directly disseminating problematic content, while those behind automated systems often escape prosecution due to the difficulty of proving a causal relationship between their actions and the resulting legal consequences. This situation confirms that Indonesia's criminal justice system remains reactive and has not yet adapted to the realities of modern digital crime.

Beyond normative issues, research also shows that the phenomenon of using bots to manipulate public opinion has equally important sociological and ethical dimensions. Bots operating on algorithmic logic can create an unrealistic social perception (artificial *consensus*), where public opinion appears to be organically formed when in fact it is the result of systematic manipulation. This phenomenon exacerbates social polarization, weakens public trust in the media, and can even trigger political tensions. In the context of digital democracy, this is particularly dangerous because it replaces public rationality with algorithmic manipulation that is difficult to detect. Therefore, criminal law must play a role not only in punishing but also in protecting the integrity of information and the public's freedom of thought from being controlled by opaque technological forces.

In the context of modern criminal law theory, extending legal responsibility to non-human entities such as algorithmic systems can be achieved through the application of the concepts of *strict liability* and *vicarious liability* [23]. Through these concepts, criminal responsibility can be imposed on the creator, controller, or party who benefits from the use of an automated system that causes legal harm [24]. Thus, the law no longer relies on the existence of malicious intent in the traditional sense, but on the consequences produced by the algorithmic action. Furthermore, corporate criminal responsibility *is* also relevant, given that most abuses of algorithms and bots are carried out by business entities or political organizations with specific economic and ideological interests [25].

The results of this study also demonstrate that protection of digital public opinion must be integrated with the principles of the right to accurate information and the right to privacy as part of human rights [26]. In this regard, criminal law can act as an *ultima ratio*,

a last resort to uphold justice when administrative regulations and social norms are no longer effective. The application of criminal sanctions for the misuse of bots and algorithms will provide a deterrent effect for perpetrators and strengthen ethical responsibility in managing digital technology. However, the application of criminal law must also maintain a balance between freedom of expression and protection against the abuse of that freedom, so that law enforcement does not become a tool to restrict freedom of expression in the digital public sphere [27].

Within a comparative legal framework, the steps taken by the European Union through the AI Act could serve as an important model for Indonesia. The regulation emphasizes the need for ethical oversight of artificial intelligence systems, including an obligation for technology providers to ensure that the algorithms they use do not pose a risk to society [28]. A similar approach could be applied in the context of Indonesian criminal law by regulating algorithmic audit mechanisms, mandatory reporting of bot usage, and imposing sanctions on parties who misuse them for manipulative purposes.

Thus, it can be concluded that the phenomenon of using algorithms and bots to manipulate public opinion demands a paradigm shift in national criminal law. The legal system, which has historically focused on human actions, needs to evolve to address the new reality, where violations can be committed by automated systems designed to mimic human behavior. Criminal law reform must be directed not only at adding articles but also at establishing a new concept of legal accountability that is responsive to the era of algorithms and artificial intelligence. Law enforcement in the digital age requires an interdisciplinary approach that combines legal, technological, and ethical aspects to ensure justice is not left behind amidst rapid technological innovation.

Ultimately, this study confirms that strengthening the legal framework regarding the use of algorithms and bots is not merely a normative necessity, but also a moral and philosophical imperative to safeguard truth, justice, and the integrity of democracy. Criminal law must be the last line of defense protecting society from the misuse of technology that threatens social order and freedom of thought. By building an adaptive and progressive legal system, Indonesia can face the challenges of the digital era while upholding the principles of justice, transparency, and legal responsibility amidst the sweeping currents of the algorithmic revolution.

## *Discussion*

The discussion of this research findings shows that Indonesian criminal law faces significant challenges in responding to the increasingly complex and dynamic development of algorithmic technology. The development of digital technology driven by artificial intelligence (*AI*) has transformed the way humans interact, communicate, and shape public opinion. However, on the other hand, this progress has also created new opportunities for crimes that are difficult to reach through traditional legal instruments [29]. In this context, the use of *bots* , namely automated, algorithm-based programs capable of duplicating messages and influencing public perception in the

digital space, has become one of the most prominent issues. This phenomenon not only impacts social and political stability but also raises serious debate in criminal law about who should be held accountable for the legal consequences of actions carried out by these non-human systems [30].

Doctrinally, classical criminal law in Indonesia is based on the principles of *actus reus* and *mens rea* , which require that actions and mistakes be committed by a legal subject with consciousness and free will [31]. However, in the context of the use of bots, most actions are carried out by an automated system that lacks moral consciousness or human will. This is where a fundamental conceptual problem arises: how can the element of fault ( *culpability* ) be proven when the perpetrator in question is not a human, but a digital entity operating based on algorithmic instructions? This question creates a dilemma in the application of traditional criminal liability principles because the law is still based on an anthropological paradigm, where only humans are considered capable of being morally and legally responsible.

To address these challenges, the concepts of corporate criminal liability and *vicarious liability* can serve as important references. Through these concepts, legal responsibility is imposed not only on the direct perpetrators but also on those who create, control, or profit from the use of bots for manipulative purposes [32]. In this context, the law can expand the scope of criminal liability to include corporations, political institutions, or parties funding bot operations with the intent of influencing public opinion. This approach is relevant considering that most bot operations in cyberspace are carried out systematically and organized by entities with specific economic or political interests. Thus, criminal responsibility does not stop at the "technical actors" alone but extends to those behind the algorithmic control structure.

In addition to conceptual issues, the research also highlights weaknesses in Indonesia's positive law, which remains sectoral and unintegrated, including Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and the New Criminal Code (KUHP). These three regulations operate in parallel without a unified legal framework that explicitly regulates algorithms, artificial intelligence, or the use of bots in the digital space [33]. Consequently, ambiguity arises in law enforcement, particularly in determining whether certain actions carried out by automated systems can be categorized as criminal offenses, and if so, who can be held accountable. This highlights the need for more specific legislative reforms, both in the form of implementing regulations and amendments to laws, that explicitly define the use of automated systems and the criminal liability arising from their use [34].

From a comparative law perspective, the European Union legal system can serve as a model because it has successfully positioned the right to accurate information and protection against digital manipulation as integral human rights. Through the Digital Services Act (DSA) and the AI Act, the EU introduced a legal framework that requires algorithmic transparency, oversight of automated systems, and the imposition of

administrative and criminal sanctions for those who use bots illegally [35]. This approach seeks to balance freedom of expression in the digital space with legal responsibility for the social impacts of technology. These principles can be adapted by Indonesia by adapting them to its national legal system, which is based on Pancasila, where the values of humanity, social justice, and moral responsibility are the primary foundations for establishing legal norms [36].

Conceptually, this discussion reinforces the urgency of implementing the principle of the right to informational *self-determination* in the digital context. When public opinion is manipulated by algorithms, the public's right to access honest and objective information is violated [37]. Algorithmic manipulation not only undermines the integrity of information but also threatens freedom of thought and expression, which are fundamental human rights. In such circumstances, criminal law serves as an instrument of public protection, both to maintain information transparency and to prevent the misuse of digital technology that can lead to social injustice. The ultima ratio theory asserts that criminal law is a last resort when social, ethical, and administrative mechanisms are no longer effective in addressing deviations. Therefore, criminal intervention against the misuse of bots and algorithms is normatively legitimate because it is directly related to the public interest and the protection of democracy.

Furthermore, this discussion emphasizes that criminal law should not be viewed solely as a means of retribution or punishment, but also as a means of prevention and social education. When the public understands that the misuse of algorithmic technology has strict criminal consequences, it will create a deterrent effect and encourage responsible use of technology. However, to achieve this, criminal law reform must be accompanied by increased capacity of law enforcement officials in understanding the workings of digital technology, including cyber forensics and algorithmic analysis. Without such increased capacity, even ideal legal norms will be ineffective in their implementation.

Thus, this discussion confirms that the application of criminal law to the use of bots to manipulate public opinion must be directed at two main objectives. First, ensuring legal accountability for parties who knowingly use algorithms to harm the public interest, whether individuals, corporations, or political institutions. Second, providing effective legal protection for the public from the risks of digital manipulation that can threaten democracy, freedom of expression, and human rights. To achieve these two objectives, it is necessary to establish legal norms that are adaptive to technological developments and based on the principles of social justice as mandated by Pancasila.

Ultimately, legal reform in Indonesia needs to be directed at integrating legal institutions and public policy so that law enforcement against algorithmic crimes can be carried out holistically. Synergy between law enforcement agencies, policymakers, academics, and civil society is absolutely necessary to ensure that regulations are not merely reactive but also preventive. This cross-sector collaboration will help create a legal system that is not left behind by technological advances but rather able to guide it toward an ethical, just, and humanitarian-oriented direction. With a comprehensive

approach, Indonesian criminal law can transform into a system that is responsive to the challenges of the algorithmic era, maintains the integrity of the digital public sphere, and protects the public from the threat of opinion manipulation in the era of artificial intelligence.

## Conclusion

Based on the research and discussion conducted, it can be concluded that the use of algorithms and bots to manipulate public opinion presents a new challenge for criminal law in the digital era. This phenomenon demonstrates a shift in the nature of crime from physical acts to crimes based on automated systems that operate through artificial intelligence and algorithms. Current Indonesian criminal law, as outlined in the Electronic Information and Transactions (ITE) Law, the New Criminal Code, and the Personal Data Protection Law, does not specifically regulate criminal liability for the misuse of algorithmic technology. Existing legal norms still focus on direct human actions, thus failing to address crimes committed with the aid of automated systems that can massively and covertly influence public perception.

Conceptually, this research emphasizes the importance of reformulating criminal law to be more adaptive to developments in digital technology. Classical legal principles such as *actus reus* (criminal act) and *mens rea* (malicious intent) need to be reinterpreted to address non-human entities such as bots and algorithms. In this context, the concepts of corporate criminal liability, strict liability, and vicarious liability become relevant to ensure that creators, controllers, and parties benefiting from the use of manipulative bots remain legally accountable. Thus, criminal law must function not only as a punitive tool but also as an instrument for prevention and protection of the public interest against the risks of information technology misuse.

Furthermore, the research findings suggest that international legal experience, such as the European Union's Digital Services Act and AI Act, can serve as important references for Indonesia in developing more comprehensive regulations regarding algorithmic accountability and transparency in digital systems. An approach that emphasizes a balance between the right to freedom of expression and protection against information manipulation can strengthen the national legal framework to better align with democratic principles and human rights.

Thus, it can be concluded that criminal law needs to expand its scope to encompass new forms of algorithm-based crimes. Strengthening legal norms, establishing independent oversight bodies, and increasing the capacity of law enforcement are strategic steps to ensure accountability in the use of digital technology. This research is expected to contribute scientifically to the development of cybercriminal law that is more responsive to technological advances, while ensuring that digital innovation is not used as a means to erode the values of truth, justice, and democratic integrity in modern society.

## References


1. I. Zaenudin and A. B. Riyan, "Perkembangan Kecerdasan Buatan (AI) Dan Dampaknya Pada Dunia Teknologi," *Jurnal Informatika Utama*, vol. 2, no. 2, pp. 128–153, Nov. 2024, doi: 10.55903/jitu.v2i2.240.
2. F. F. Syam, "Efek Polarisasi Algortima Media: Analisis Teori Power Dan Knowlegde Michel Foucault," *RIGGS: Journal of Artificial Intelligence and Digital Business*, vol. 4, no. 2, pp. 3424–3531, Jun. 2025, doi: 10.31004/riggs.v4i2.1070.
3. A. Nuryanto, A. Kebijakan pada Biro Kerja Sama dan Hubungan Masyarakat, S. Jenderal, K. Pendidikan, and R. dan Teknologi, "Tantangan Administrasi Publik di Dunia Artificial Intelligence dan BOT Public Administration Challenges in the World of Artificial Intelligence and BOT," 2020.
4. G. Dzunuwanus, "MANIPULASI NARASI PUBLIK MELALUI AKUN BOT DALAM AKTIVISME DIGITAL PRO-IKN DI MEDIA SOSIAL X," *Journal of Politic and Government Studies*, vol. 14, no. 3, 2025.
5. I. Z. Al Fatih, "Peran Media Sosial dalam Kampanye Politik di Indonesia Lima Tahun Terakhir: Antara Demokrasi dan Manipulasi Informasi," *COMSERVA : Jurnal Penelitian dan Pengabdian Masyarakat*, vol. 4, no. 7, pp. 2227–2237, Nov. 2024, doi: 10.59141/comserva.v4i7.2611.
6. "Peran Algoritma Media Sosial dalam Penyebaran Propaganda Politik Digital Menjelang Pemilu," *Jurnal Kajian Stratejik Ketahanan Nasional*, vol. 7, no. 1, Jun. 2024, doi: 10.7454/jkskn.v7i1.10090.
7. H. Suriadi, "Krisis Kepercayaan Masyarakat terhadap Lembaga Publik di Era Disinformasi Digital," *Journal of Social, Educational and Religious Studies*, vol. 1, no. 1, 2025, [Online]. Available: https://jurnal.suriaacademicpress.com/index.php/jsers
8. D. R. Fatmala, A. Amelia, and F. A. Trianingsih, "The Use of Social Media Bot Accounts on Influencing Public Opinion: A Legal Review in Indonesia," *Legality: Jurnal Ilmiah Hukum*, vol. 28, no. 2, pp. 169–182, Sep. 2020, doi: 10.22219/ljih.v28i2.12148.
9. Fransiskus Nomor, Ida Bagus Anggapurana Pidada, and Kadek Fredi Andrika Adnantara, "Penegakan Hukum Terhadap Penyalahgunaan Sosial Media dalam Membangun Opini Publik pada Pemilu 2024," *Jembatan Hukum : Kajian ilmu Hukum, Sosial dan Administrasi Negara*, vol. 1, no. 3, pp. 308–326, Jul. 2024, doi: 10.62383/jembatan.v1i3.572.
10. Cheny Berlian, "Kejahatan Siber Yang Menjadi Kekosongan Hukum," *JOURNAL EQUITABLE*, vol. 5, no. 2, pp. 19–20, Apr. 2021, doi: 10.37859/jeq.v5i2.2532.
11. A. A. Respati, "Reformulasi UU ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation," *JURNAL USM LAW REVIEW*, vol. 7, no. 3, pp. 1737–1758, Dec. 2024, doi: 10.26623/julr.v7i3.10578.
12. M. Kossay and M. F. Idris, "Tanggung Jawab Hukum Platform Digital Atas Penyalahgunaan Ai Dalam Transaksi Elektronik," *MAGISTRA Law Review*, vol. 6, no. 01, p. 44, Mar. 2025, doi: 10.56444/malrev.v6i01.5879.
13. Moch. M. Taufiqurrohman and Gultom. Elisatri, "Corporate Digital Responsibility: Tanggung Jawab Etis Penggunaan Teknologi Digital dalam Bisnis Perusahaan," *Humani (Hukum dan Masyarakat Madani)*, vol. 13, no. 2, May 2023.
14. H. S. Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review*, vol. 24, no. 2, pp. 289–304, Nov. 2022, doi: 10.37253/jjr.v24i2.7280.
15. S. A. Wiraguna, "Metode Normatif dan Empiris dalam Penelitian Hukum: Studi Eksploratif di Indonesia," *Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum*, vol. 3, no. 3, Nov. 2024, doi: 10.59818/jps.v3i3.1390.
16. R. Tahir, *METODOLOGI PENELITIAN BIDANG HUKUM : Suatu Pendekatan Teori dan Praktik*. Jambi: Sonpedia Publishing Indonesia, 2023.
17. K. Benuf and M. Azhar, "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan*, vol. 7, no. 1, pp. 20–33, Apr. 2020, doi: 10.14710/gk.2020.7504.
18. D. O. Susanti, *Penelitian Hukum: Legal Research*. Jakarta: Sinar Grafika, 2014.
19. Q. Arifuddin, *Metodologi Penelitian Hukum*. Jambi: Sonpedia Publishing Indonesia, 2025.
20. B. Raharjo, *Teori Etika Dalam Kecerdasan Buatan (AI)*. Semarang: Yayasan Prima Agus Teknik, 2023.
21. M. Bahram, "Tantangan Hukum Dan Etika (Rekayasa Sosial Terhadap Kebebasan Berpendapat Di Dunia Digital)," *SENTRI: Jurnal Riset Ilmiah*, vol. 2, no. 12, pp. 5092–5109, Dec. 2023, doi: 10.55681/sentri.v2i12.1895.

22. Wahyudi, "Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI," *INNOVATIVE: Journal Of Social Science Research*, vol. 5, 2025.
23. A. Sofian, "Konsepsi Subjek Hukum dan Pertanggungjawaban Pidana Artificial Intellegence," *Halu Oleo Law Review*, vol. 9, no. 1, pp. 13–26, Mar. 2025, doi: 10.33561/holrev.v9i1.129.
24. F. Fatimah, "Pertanggungjawaban Pengganti (Vicarious Liability) Dalam Kebijakan Formulasi Hukum Pidana Di Indonesia," *LAW REFORM*, vol. 7, no. 2, p. 1, Oct. 2012, doi: 10.14710/lr.v7i2.12408.
25. A. Situmeang, N. C. Weley, and H. S. Disemadi, "Kepastian Pertanggungjawaban Hukum Pidana Korporasi atas Penyalahgunaan Data Pribadi di Indonesia," *Proceedings Series on Social Sciences & Humanities*, vol. 23, pp. 8–15, Jun. 2025, doi: 10.30595/pssh.v23i.1544.
26. N. Putu Rai Yuliartini, L. Norman Kbarek, and S. Monteiro, "MEDIA HUKUM From Retribution to Restoration: Human Rights-Based Legal Protection for Women Victims of Sexual Violence," *Nationally Accredited Journal*, vol. 32, no. 2, 2025, doi: 10.18196/jmh.v32i2.26214.
27. N. P. Rai Yuliartini, D. G. Sudika Mangku, and L. N. Kbarek, "Customary law and justice: Protecting the rights of women victims of sexual violence in Bali," *Jurnal Hukum Novelty*, vol. 15, no. 2, pp. 180–199, Oct. 2024, doi: 10.26555/jhn.v15i2.28542.
28. K. B. Kirana and W. Silalahi, "Tantangan Regulasi Kecerdasan Buatan (AI) dalam Perspektif Hukum Perlindungan Data Pribadi di Indonesia," *Cerdika: Jurnal Ilmiah Indonesia*, vol. 5, no. 6, pp. 1807–1817, Jun. 2025, doi: 10.59141/cerdika.v5i6.2711.
29. D. Sulistyawati Handayani, R. Kaunang, S. Sondang, and I. Irwansyah, "Manfaat dan Potensi Masalah Penggunaan Kecerdasan Buatan (AI) dalam Komunikasi Publik," *Co-Value Jurnal Ekonomi Koperasi dan kewirausahaan*, vol. 14, no. 12, May 2024, doi: 10.59188/covalue.v14i12.4334.
30. D. G. S. Mangku, N. P. R. Yuliartini, I. N. Suastika, and I. G. M. A. S. Wirawan, "The Personal Data Protection of Internet Users in Indonesia," *Journal of Southwest Jiaotong University*, vol. 56, no. 1, 2021, doi: 10.35741/issn.0258-2724.56.1.23.
31. D. L. B. Njoto, "Rekonstruksi Asas Actus Non Facit Reum Nisi Mens Rea dalam Tindak Pidana," *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, vol. 7, no. 3, pp. 3344–3355, Mar. 2024, doi: 10.54371/jiip.v7i3.3735.
32. Nazifah, D. G. S. Mangku, and N. P. R. Yuliartini, "Fulfillment of Labor Rights for Persons with Disabilities in Indonesia," *Int J Criminol Sociol*, vol. 10, pp. 272–280, Feb. 2021, doi: 10.6000/1929-4409.2021.10.33.
33. D. G. Sudika Mangku and K. Astiti Narayani, "The Dangers of The Crime of Genocide: International Law Review," *Journal of Judicial Review*, vol. 24, no. 1, pp. 81–90, Jun. 2022, doi: 10.37253/jjr.v24i1.6467.
34. N. P. R. Yuliartini, "LEGAL PROTECTION FOR VICTIMS OF CRIMINAL VIOLATIONS (CASE STUDY OF VIOLENCE AGAINST CHILDREN IN BULELENG DISTRICT)," *Veteran Law Review*, vol. 2, no. 2, p. 30, Nov. 2019, doi: 10.35586/velrev.v2i2.1241.
35. R. Hartono, S. Efendi, E. Pratiwi, and J. Khan Haikal, "Analisis Yuridis Terhadap Tanggung Jawab Layanan Chatbot Berbasis Ai Dalam Pelindungan Konsumen Di Era Digital," *Jurnal Restorative Justice*, vol. 1, no. 1, 2025, [Online]. Available: https://jurnal.umkal.ac.id/index.php/rj
36. Raisa Safina, Khalda Alifia Azzahra, and Ananda Fersa Dharmawan, "Kajian Yuridis Penggunaan Kecerdasan Artifisial pada Pembuatan dan Penyebaran Konten Pornografi di Media Sosial dalam Hukum Positif Indonesia," *Mandub : Jurnal Politik, Sosial, Hukum dan Humaniora*, vol. 2, no. 1, pp. 302–313, Dec. 2023, doi: 10.59059/mandub.v2i1.918.
37. N. Remolina and M. J. Findlay, "The Paths to Digital Self-Determination - A Foundational Theoretical Framework," *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3831726.