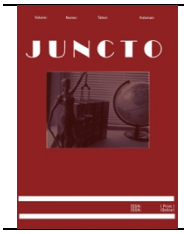

JUNCTO: Jurnal Ilmiah Hukum, 7(2) 2025: 244-254
DOI: 10.31289/juncto.v7i2.6849

JUNCTO: Jurnal Ilmiah Hukum

Available online http://jurnalmahasiswa.uma.ac.id/index.php/juncto
Diterima: 2025-11-28; Direview: 2025-12-19; Disetujui: 2025-12-30

Digital Criminalisation: The role of Electronic Evidence in the 17 + 8 Demonstration

Emilia Metta Karunia Wijaya
Program Studi Ilmu Hukum, Fakultas Hukum dan Komunikasii
Uversitas Katolik Soegijapranata Semarang, Indonesia

Abstract

This article examines the role of electronic evidence and the practice of digital criminalisation in the series of demonstrations in response to 17+8 people's demands. The purpose of this study is to analyse the position of electronic evidence in proving criminal acts in the series of protests 17+8 of people's needs, the application of the ITE Law to the digital activities of the 17+8 demonstrations in the context of digital criminalisation, and the adequacy of legal norms in protecting freedom of expression in the digital era. The research uses a normative juridical method with a case study approach to examine the practice of digital criminalisation during a series of demonstrations. This study highlights an ambivalence in the use of electronic evidence. While it serves as a tool for accountability, it is also weaponized through the ITE Law's vague provisions to repress dissent. Consequently, Indonesia's legal framework remains focused on maintaining public order rather than safeguarding the fundamental rights of demonstrators. This article recommends reformulating the ITE Law's provisions on rubber articles, strengthening the implementation of the PDP Law, and establishing an independent institution to oversee the protection of personal data and digital restrictions.

Keywords: Electronic Evidence; Digital Criminalisation; ITE Law

How to Cite: Wijaya, E.M.K., (2025), Electronic Evidence and Digital Criminalisation in the 17 + 8 People's Demands Demonstration, *JUNCTO: Jurnal Ilmiah Hukum, 7(2) 2025: 244-254*

**E-mail: emiliawijaya96@gmail.com* *ISSN 2550-1305 (Online)*

INTRODUCTION

Demonstrations took place simultaneously in various regions from August 25, 2025, to August 31, 2025. This mass action originally started when the House of Representatives (DPR) was insensitive to the suffering of the people and instead danced happily over a fantastic housing allowance. In response to this injustice, people used demonstrations as a means of political participation to channel their aspirations and safeguard democratic life. Calls for demonstrations first appeared in chain messages demanding the investigation of the alleged corruption case involving former president Joko Widodo's family, the impeachment of Vice President Gibran Rakabuming Raka, and urging the DPR to carry out its functions and duties as a government control (Mardianti 2025).

Initially, the demonstrations were peaceful on 25-28 August 2025, but the DPR did not meet with the masses. In the evening on August 28, 2025, the Demonstration became chaotic. The peak was when Affan Kurniawan, an online motorbike taxi driver, was killed by a Brimob tactical vehicle, which then sparked public anger. Amid the heat of the situation, several board members went on holiday abroad. This further fuelled the anger of the masses, and clashes between police and demonstrators were inevitable. The chaos spread to various regions, resulting in the burning of several public facilities and the ransacking of the houses of members of the House of Representatives. The escalation of the 17+8 People's Demands demonstrations marked a shift from economic unrest to a broader social and political agenda. These demonstrations then developed into a political momentum involving various elements of society, ranging from students, workers, activists, and professional groups.

The 17+8 demonstrations of the people's demands were not only held in physical spaces such as the DPR Building and the police station, but also penetrated the digital space. Social media, streaming channels, and video uploads became a medium for documentation, mass organisation, and monitoring of the action. Digital space expands the impact of demonstrations and can become an alternative participation space. Information uploaded by protesters is consumed not only by people at the demonstration site and the public, but also by people in various locations. Videos of apparatus violence, political statements, and photos of speeches spread widely in just seconds. This shows that contemporary demonstrations are no longer local, but have national and transnational dimensions. However, this development also presents new challenges, as digital activities during demonstrations are prone to manipulation and are even used to criminalise demonstrators.

The case of Delpedro Marhaen, Executive Director of Lokataru Foundation, is an important illustration. Delpedro's detention on charges of provoking anarchist acts in the field and of calling for demonstrations through social media (Kharismaningtyas, 2025) shows that posts, invitations, and statements of attitude in the digital space can create loopholes for criminalisation. A similar pattern was also seen in the case of Khariq Anhar, a student activist from Riau who became a suspect and was detained at Polda Metro Jaya. Khariq was detained for satire or jokes about the action plan posted on his Instagram account @aliansimahasiswapenggugat (Siregar 2025). This phenomenon does not stop at the individual level, but is reflected in broader data. Andhyta F. Utami, an activist who submitted the 17+8 people's demands document to the House of Representatives, noted that there were 11 fatalities, around 500 people were injured, and 3,400 people were criminalised in this series of demonstrations (Fadilah, 2025). This data does not specify the number of people arrested for digital activities, but it shows that democratic practices in Indonesia still face serious problems. Where the mechanism of community political participation is anticipated in the context of repressive actions. Activities in the digital space are

now treated as equal to activities in the physical space, thus strengthening the urgency of discussing electronic evidence and the limits of criminalisation in the digital world.

The Criminal Procedure Code categorises evidence as witness testimony, expert testimony, letters, instructions, and the accused's testimony. Technological developments have introduced new evidence regulated in Article 1 of Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 1 of 2008 concerning Electronic Information and Transactions. Article 1 of the Law explicitly recognizes Electronic Information and/or Electronic Documents, and their printouts, as legal evidence under the applicable Law of Procedure in Indonesia. New types of evidence that can be classified as electronic evidence, such as e-mail, witness examination using videoconference, and telecomfence in the form of Google Meet, Zoom, Skype, Microsoft Teams, and so on, short message service systems, hidden cameras or CCTV recordings, and other electronic media as a medium for data storage (Asimah, 2020).

Electronic evidence must still fulfil several requirements to be accepted in court. The integrity of electronic evidence must be guaranteed through a certified information security system to safeguard its content (Suryana & Sakmaf 2025). Electronic evidence plays a dual role in the 17+8 demonstrations of popular demands. Electronic evidence documenting the authorities' violence can constitute evidence of human rights violations. Conversely, electronic evidence can also be used to criminalise protesters. This is the ambivalence of electronic evidence: an instrument of justice and a potential tool of repression.

The phenomenon of digital criminalisation is increasingly evident in demonstrations. The actions that have been taking place since August 25, 2025, are not only marked by allegations of human rights violations against participants but also have a massive impact on the digital rights of internet users in Indonesia. SAFEnet, as an organisation that fights for digital rights, sees this situation as a clear manifestation of restrictions on freedom of expression, digital authoritarianism, and the militarisation of Indonesia's cyberspace (SAFEnet, 2025). During the 17+8 Demonstration, several protesters reportedly faced digital-based intimidation. Some of their social media accounts were hacked, and their posts were used to support police reports.

Some of the events that showed serious violations of citizens' digital rights during the demonstrations were the criminalisation of student activist Khariq Anhar, who was the manager of the Aliansi Mahasiswa Penggugat (AMP) social media account; the circulation of WhatsApp contacts of several civil society coalition activists; the disruption of internet access and information in digital spaces; the suspension of TikTok's live streaming feature; indications of an information operation to divert public attention from the issue of police violence; statements from the Ministry of Communications and Digital regarding plans to summon representatives of Meta and TikTok; and the police's seizure, search, and data siphoning of mobile phones of protesters in Bali (SAFEnet, 2025). This situation shows a pattern of using the ITE Law to digitalise criminalisation. Instead of protecting the public from cybercrime, ITE Law is used to silence political criticism.

Digital criminalisation has profound implications for democracy. It will result in widespread apathy, weak public control, and the posture of undermining legal legitimacy. The problem is that the ITE Law contains several articles that have been interpreted differently since its implementation. The scope of Article 28, paragraph (3) of the ITE Law on false notifications that cause riots and the provisions on public order in Article 40 are often used selectively to ensnare activists and people who criticise the government.

Normatively, the right to freedom of expression is guaranteed in Article 28E of the 1945 Constitution, which states that everyone has the right to freedom of association, assembly, and expression. This guarantee is strengthened by Law No. 39/1999 on Human Rights and the

ratification of the International Covenant on Civil and Political Rights (ICCPR) through Law No. 12/2005. Thus, freedom of expression is a fundamental right that must be protected. In reality, there is a gap between legal norms and their implementation. Electronic evidence, which should be a tool to ensure accountability, is often used to justify repression.

This research is essential to examine the position of electronic evidence in proving criminal acts in the series of demonstrations on 17+8 people's demands; the application of the ITE Law to the digital activities of the 17+8 demonstrations in the context of digital criminalisation; and the adequacy of legal norms in protecting freedom of expression in the digital era. Based on the description above, it is clear that electronic evidence and digital criminalisation in the 17+8 People's Demands demonstration are urgent legal issues that warrant study. This phenomenon shows how the digital space opens up opportunities for democracy while creating the risk of criminalisation. In contrast to previous studies that focused on cybersecurity, this article uses the 17+8 incident to examine how electronic evidence was used to criminalize activists. Primarily, no research has specifically addressed the 17+8 People's Demands demonstrations as a case study.

METHODS

This research uses a normative legal approach as its primary approach, along with a case approach. The normative legal approach is carried out through a review of theoretical concepts, legal principles, and legislation related to this study (literature or secondary materials) (Muhaimin, 2020). The normative juridical approach was chosen because the research focuses on the study of positive legal norms governing the position of electronic evidence in criminal procedural law and Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024. The case approach is used to examine the practice of digital criminalisation that occurred during the series of demonstrations under the 17+8 People's Demands, to understand the relationship between legal norms and their implementation.

The analysis is conducted through a prescriptive-argumentative approach to critically evaluate the gap between legal norms and the practice of digital criminalization. The research data consists of primary legal materials, including laws and regulations, and secondary legal materials, including journals, scientific articles, NGO reports, media analysis, and expert opinions. The data were collected through a literature review and analysed qualitatively by interpreting legal regulations and empirical facts from a series of digital criminalisation cases at the 17+8 Demonstration of people's demands. Qualitative analysis was conducted to examine the position of electronic evidence in proving criminal acts in the series of protests of 17+8 people's needs; the application of the ITE Law to the digital activities of the 17+8 demonstrations in the context of digital criminalisation; and the adequacy of legal norms in protecting freedom of expression in the digital era.

RESULT AND DISCUSSION

The Position of Electronic Evidence in Proving Criminal Acts in the Series of Demonstrations of 17+8 People's Demands

As stipulated in Article 1, paragraph (3) of the Constitution of the Republic of Indonesia, Indonesia is a state of law. Within this framework, the law provides behavioural guidelines in the form of legal norms (Dirjosisworo, 2018). Every individual who commits an offence under criminal law can then be examined in court to prove their guilt or innocence of the alleged act (Prinst, 2022).

Evidence plays a fundamental role in obtaining the truth. In the legal context, proof is essential to find the truth of a legal event with legal consequences (Mansyah et al. 2023). In criminal procedure law, evidence is a provision that limits court proceedings in an effort to seek and defend the truth. Both judges and public prosecutors, as well as legal counsel and defendants, are bound by the provisions of the procedure and assessment of evidence determined by law (Harahap n.d.).

Article 184 paragraph (1) of KUHAP mentions the types of evidence that are valid and can be used in court: witness testimony, expert testimony, letters, instructions, and the defendant's testimony. The judge can only use these five pieces of evidence in making a decision. This is because Indonesia adheres to the Negatief Wettelijk Bewijstheorie evidentiary system. The Negatief Wettelijk Bewijstheorie represents a different perspective, in which the judge's belief arises from the evidence presented in accordance with the law. This theory focuses on the judge's conviction derived from legal evidence (Gea 2024). Bewijsvoering concerns how evidence is presented in court, a concept of particular importance in systems following the due process model of criminal justice. It emphasizes formalistic or procedural aspects, though in the realm of electronic crime, its relevance may be limited (Kurniawan 2019).

Negatief: Wettelijk Bewijstheorie plays a vital role in ensuring legal certainty, because in this closed system, judges can only use valid evidence in accordance with the law. However, this system is not responsive enough to technological developments. The regulation of types of evidence in the Criminal Procedure Code, passed in 1981, could not anticipate the birth of electronic evidence. As a result, the provisions of Article 184 of the Criminal Procedure Code face severe challenges due to the increasing number of criminal incidents that leave digital traces.

Information and communication technology development also significantly affects the criminal procedure law. Legal facts previously only recorded through direct testimony, written documents, or conventional instructions can now be captured and documented through digital media. Video recordings, social media posts, short messages, and other online documentation have become integral. The role of electronic evidence in proving criminal offences in the context of 17+8 demonstrations of people's demands is essential, as protests are carried out in both physical and digital spaces. This condition then encourages the birth of special rules that recognise electronic evidence as part of the evidentiary system.

The juridical recognition of electronic evidence was first explicitly regulated in Article 5, paragraph (1) of Law No. 11 of 2008 concerning ITE. The article states that electronic information/or electronic documents, and their printouts, are valid legal evidence. Meanwhile, Article 5, paragraph (2), of the ITE Law regulates electronic information and/or electronic documents, which constitute an extension of legal evidence in accordance with the applicable procedural law in Indonesia. Law No. 1 of 2024, the second amendment to the ITE Law, reaffirms the recognition of electronic evidence in Article 5 of Law No. 11 of 2008 concerning ITE.

The admission of electronic evidence in KUHAP is lex generalis, while the ITE Law is lex specialis, because its rules regulate more specific regulations. Although the Criminal Procedure Code has not been revised to date, electronic evidence can be recognized under the lex specialis derogat legi generali mechanism. This means that the ITE Law, as a special law, can expand the evidentiary position as regulated in Article 184 of the Criminal Procedure Code. However, in its proof, it still adheres to the negative proof system (negatief wettelijk) as stipulated in Article 183 of the Criminal Procedure Code, which requires the judge to base his decision on at least two valid pieces of evidence.

The position of electronic evidence in the context of the Demonstration of 17+8 people's demands is recognised as valid evidence. The recognition of electronic evidence allows the court

to obtain a more comprehensive picture of the facts presented in demonstration video recordings, social media posts, and circulating messages. This electronic evidence can serve as an instrument of public accountability, recording the authorities' actions, documenting the course of action, and storing event data. Electronic evidence can be used in criminal proceedings. This evidence can reveal the mistakes of the apparatus, for example, the case of online motorbike taxi drivers and other repressive actions of the apparatus. In addition, electronic evidence can also be used to prove alleged criminal offences committed by demonstrators.

However, the reliability of electronic evidence is still determined by how it is obtained. The principle of due process of law requires that electronic evidence be obtained legally, not through hacking or illegal seizure. Electronic evidence must also meet technical standards that guarantee its authenticity and security. The international standard ISO/IEC 27037:2012 confirms that digital evidence must fulfil the elements of authenticity, integrity, and reliability. Authenticity means that the data comes from a legitimate source, and integrity requires that the content and metadata remain unchanged from the time it is obtained until it is presented in court. At the same time, reliability demands accountable acquisition and storage methods (ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence). Furthermore, the standard also emphasises the importance of the chain of custody principle, namely the chronological recording of each stage of handling digital evidence, from identification, collection, acquisition, to preservation. Thus, the fulfilment of the elements of authenticity, integrity, reliability, and the application of the chain of custody make electronic evidence have strong legitimacy as legal evidence in court (ISO/IEC 27037:2012 – Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence 2012).

In the context of the Demonstration of 17+8 people's demands, electronic evidence plays a strategic role, as almost all the dynamics of the event are recorded on digital media. Video recordings, social media posts, and other electronic documents can be used as evidence to prove criminal offences. Normatively, the position of electronic evidence in the 17+8 Demonstration is that it is a legitimate instrument that expands the evidentiary system and is relevant to the dynamics of events. However, issues related to how the evidence is used in practice will be further analysed in the following problem formulation.

The Application of ITE Law to Digital Activities in the 17+8 Demonstration in the Context of Digital Criminalisation

Applying the ITE Law shows ambivalence in the demonstrations of 17+8 people's demands. Articles in the ITE Law that should be used to protect people from cybercrime are instead used to silence criticism. This is reflected in several cases that have ensnared activists and academics. Depeldro, as director of Lokataru Fondation; Muzaffar Salim, as staff of Lokataru Fondation; Syahdan Husein, an activist of Gejayan Memanggil; Khariq Anhar, a student activist from Riau University; Figha Lesmana, an alumnus of Bung Karno University; and someone with the initials RAP were charged.

The six suspects were prosecuted using Article 160 of the Criminal Code (KUHP) and/or Article 45A paragraph 3 in conjunction with Article 28 paragraph (3) of Law No. 1 of 2024 concerning ITE and/or Article 76H jo. Article 15 jo. Article 87 of Law No. 35 of 2014 on Child Protection, Articles in the ITE Law, initially designed to protect the public from cybercrime, have instead become instruments for silencing criticism (Azzahra, 2025). Criticism that should be legitimate as a form of citizen political participation is treated as a criminal offence.

One of the posts used as evidence by the police belongs to the @lokatarufoundation account. The account posted a photo containing information about a complaint post for students who wanted to participate in a demonstration on August 28, 2025. The photo reads "Are you a student? Want to demonstrate? Already demonstrated? Threatened with sanctions? Or already sanctioned? Let us fight together! #jangantakut" (Azzahra, 2025). The substance of the upload is information about the Demonstration and an invitation to escort the action peacefully, but it is considered a form of incitement. The widespread interpretation shows how the ITE Law is used against its original purpose. These articles have repeatedly been used to ensnare activists in the series of demonstrations of 17+8 people's demands.

In the case of Khariq Anhar, a student from Riau who was named a suspect due to a satirical post on the Instagram account @aliansimahasiswapenggugat, Khariq used the method of overwriting the photo's text to replace the title with Said Iqbal. He affirmed that Anarcho, Students, and BEM immediately joined the August 28 Action: This is a Pure Movement of the Indonesian People! (Azzahra 2025) The post was actually a satirical joke about the action plan, but the authorities treated it as a real provocation that had the potential to cause unrest. The application of articles of the ITE Law in the context of the 17+8 Demonstration is clearly not aimed at protecting digital rights but rather at criminalising political activity in cyberspace.

The disruption of internet access at several action points, the suspension of TikTok's live broadcast feature, and the hacking of activists' social media accounts are evidence that restrictions on digital space are being carried out systematically. On 28-31 August 2025, people complained about difficulties accessing social media, which led to the obstruction of information about the Demonstration. This was exacerbated by the termination of TikTok Live on the evening of August 30, 2025. In fact, the TikTok Live feature was used to record several vital events during the demonstrations. Southeast Asia Freedom of Expression Network (SAFEnet) suspects that several acts of digital repression have occurred since the August 25, 2025, incident. This included internet slowdowns that happened at several action points. SAFENet also noted that many accounts were suspended and posts related to police violence were taken down under the pretext of incitement and violence (Fitriansyah 2025).

This phenomenon shows that restrictions on digital space are technical, systematic, and targeted. However, the fundamental problem is the absence of a clear legal basis that authorises the government and law enforcement officials to take such actions. Article 40, paragraph (2) of Law No. 11 of 2008 on ITE, as amended by Law No. 1 of 2024, regulates the government's obligation to protect the public interest from all types of disturbances as a result of the misuse of electronic information and electronic transactions that disturb public order. However, the ITE Law and its amendments do not elaborate further on the form of protection in question or how the provisions of the article are implemented. This article is general and is often used by the government as a basis for implementing digital restriction measures, ranging from slowing down the internet to reducing content on social media.

The interpretation of the articles in the ITE Law clearly violates the principle of the rule of law as stipulated in Article 1, paragraph (3) of the 1945 Constitution. Any restriction on the people's rights violates the right to freedom of association, assembly, and expression as stipulated in Article 28E of the 1945 Constitution. This guarantee is strengthened by Law No. 39/1999 on Human Rights and by the International Covenant on Civil and Political Rights (ICCPR), which was ratified through Law No. 12/2005. The ITE Law, in its implementation, negates these guarantees. Apparatus repression reflects the excessive and disproportionate use of the law. Criticism in the digital space is often seen as a violation of public order and provocation rather than as a form of democracy.

This condition shows a structural bias in the use of electronic evidence. This bias has ultimately led to the practice of interpreting articles in the ITE Law that are not in accordance with the principles of the rule of law. Normatively, electronic evidence is recognised as legal evidence through Article 5 of the ITE Law. Supposedly, this provision can be used to reveal violations committed by the authorities, such as violence against demonstrators or excessive force. However, in practice, electronic evidence is used selectively. Video recordings showing tear gas shootings, mistreatment, and negligent homicide by police officers during the 17+8 demonstrations of people's demands were not followed up on in the criminal realm. The repressive actions of police officers are only subject to professional code of ethics sanctions and internal disciplinary penalties, which only strengthen the impunity of police officers. In contrast, activists' social media posts that contain criticism or satire are immediately used as grounds for arrest.

The structural bias in using electronic evidence in the 17+8 demonstrations of people's demands has profound implications for the destruction of democracy. The detention of activists for social media posts has led to public fear of voicing their opinions. Meanwhile, the impunity obtained by police officers has actually resulted in strengthened repression practices. Internet throttling, account hacking, and digital criminalisation will continue without strict sanctions. This condition will certainly undermine public trust in the police institution, eroding freedom of expression and the right to information.

The blocking of TikTok's live-streaming feature and internet disruptions during the 17+8 demonstrations of people's demands also hindered transparency. Demonstrations that should have been monitored by the public and were meant to foster openness were dominated by the official government narrative. This is contrary to the principle of transparency, a characteristic of a democratic state. Seeing the criminalisation loopholes in applying the ITE Law to the 17+8 Demonstration of people's demands, strategic steps are needed to prevent similar behaviour. This step can begin by reformulating articles in the ITE Law that are open to multiple interpretations. This phrase does not specify the form of action the government can take, so it is prone to misuse as a basis for legitimising repression. Article 40 of the ITE Law contradicts the principle of legality in criminal law because it opens the door to subjective interpretations prone to misinterpretation. The government can call criticism a 'public order disturbance' to justify repressive action. The second step can begin with the government recognizing digital rights as integral to freedom of expression. Disconnecting from the internet or blocking digital platforms should not be done arbitrarily, especially to limit public transparency. This is because the right to freedom of expression and information is an inherent human right that the Constitution must protect.

The Adequacy of Legal Norms in Protecting Freedom of Speech in the Digital Age

The freedom to obtain information and express opinions is a constitutional right explicitly guaranteed by the 1945 Constitution. As explained in the previous discussion, Article 28, E, paragraph (3), of the 1945 Constitution protects the right of every person to freedom of association, assembly, and expression. Meanwhile, Article 28F of the 1945 Constitution has guaranteed the right to communicate and convey information through all types of channels. These two articles in the 1945 Constitution are the pillars of public protection for communicating, obtaining, and expressing opinions in the digital space.

Today's digital space is a space for public participation, where various information can be conveyed quickly. People use digital media to express criticism, opinions, and political aspirations. Digital media refers to a broad spectrum of content and information that is

transmitted and stored in digital formats, encompassing text, images, audio, video, and interactive elements (Negi & Akanksha, 2024). At its core, digital media leverages digital technologies to capture, process, and disseminate data, making it easily accessible and distributable through electronic devices and the Internet (Negi & Akanksha, 2024). Digital media, especially social media, can be used as an effective and innovative mobility effort to mobilize the community, including the masses, in the 17+8 demonstrations of people's demands.

Using digital space to foster community participation cannot be separated from legal norms that guarantee freedom of speech. Freedom of speech is not only protected by the Constitution, but also strengthened by various legal regulations. Law No. 39/1999 on Human Rights has affirmed the state's obligation to guarantee citizens' human rights, including the right to freedom of expression. Indonesia has also ratified the International Covenant on Civil and Political Rights (ICCPR) through Law No. 12 of 2005. Article 19 paragraph (1) and Article 19 paragraph (2) of the ICCPR stipulate that everyone has the right to freedom of opinion and expression, including seeking, receiving, and conveying information in any form without interference.

The enactment of Law No.27 of 2022 on Personal Data Protection (PDP Law) confirms that personal data is a fundamental right that must be protected. The PDP Law protects the right of data subjects to control the use of personal information, protects the privacy of data owners, regulates the obligations of data controllers, and stipulates sanctions. These arrangements show that adequate protection has been provided through constitutional guarantees and existing legal regulations. The government has also facilitated the utilisation of information and electronic transactions by taking into account applicable laws and regulations (Budhijanto, 2024).

Democratic principles have also underlined the right of every individual to express opinions and actively participate in public discussions without fear of reprisal, intimidation, or persecution (Andersen, 2022). Freedom of speech allows people to voice their ideas, criticisms, and aspirations, contributing to more inclusive and accountable decision-making. By engaging in the decision-making process, people are concerned with outcomes and have confidence in the democratic system (Xiang, 2024).

Unfortunately, although this freedom of expression has been regulated, it still faces challenges in practice. The criminalisation of demonstrators who are demanding 17+8 people's rights still occurs. Several demonstrators were arrested and charged with the criminal offence of provocation. Mobile phones belonging to demonstrators were confiscated, and their browsing history was viewed without their consent. Protecting demonstrators' personal data against apparatus actions, such as confiscating mobile phones, digital searches, or forced data siphoning, has not been explicitly guaranteed. This violates demonstrators' human rights and their right to data privacy. The PDP Law has not prevented digital criminalisation. Although a data protection supervisory authority is in place, it has yet to be fully established. In addition, no independent institution is authorised to oversee platform blocking and activist account hacking. All authority is in the hands of the government and its apparatus, potentially leading to abuse of power. This is undoubtedly contrary to the principle of the rule of law, which requires supervision of any restrictions on citizens' rights.

Using articles in the ITE Law also strengthens the practice of digital criminalisation. As explained in the second discussion, articles in the ITE Law are often used to ensnare activists. Some articles in the ITE Law are multi-interpretive, while the protection of digital rights receives little attention. As a result, although electronic evidence has been recognised as valid, it is used to strengthen digital criminalisation. Meanwhile, electronic evidence that shows repressive actions by the authorities is often ignored.

Articles with multiple interpretations have the potential to make Indonesian regulations more often used as instruments of restriction rather than legal protection, in contrast with international standards that place human rights at the center. The European Union has gone further with the General Data Protection Regulation (GDPR), which places personal data protection as a fundamental right. Article 1 of the GDPR contains the Following rules relating to the protection of natural persons regarding the processing of personal data and the free movement of personal data. Even at the Southeast Asian level, the Manila Principles on Intermediary Liability provide concrete guidance to prevent arbitrary restrictions on freedom of expression online (Principles n.d.). Compared with the GDPR and the Manila Principles on Intermediary Liability, Indonesia's legal norms appear more defensive, emphasising public order over the protection of citizens' rights. The emphasis on the phrase' public order' without specifically explaining what it means makes this article multi-interpretive.

Digital criminalisation can be prevented by reformulating articles in the ITE Law that are open to multiple interpretations. The formulation of the rubber articles in the ITE Law needs to be clarified to avoid ensnaring people's political expression. Criticism, satire, and suggestions must be treated as freedom of expression, not criminal offences. Strengthening the implementation of the PDP Law is essential to protect the political rights of demonstrators. For example, the confiscation of mobile phones or the siphoning of personal data by the authorities should be carried out only with the court's permission and under the supervision of an independent institution. In addition, a personal data protection authority must be established immediately to ensure adequate supervision. The personal data protection authority will oversee internet disconnection, content removal, and platform blocking policies. Without the supervision of an independent institution, police officers can take repressive actions arbitrarily under the pretext of maintaining public order.

Digital criminalisation can be prevented by reformulating articles in the ITE Law that are open to multiple interpretations. The formulation of the rubber articles in the ITE Law needs to be clarified to avoid ensnaring people's political expression. Criticism, satire, and suggestions must be treated as freedom of expression, not criminal offences. Strengthening the implementation of the PDP Law is essential to protect the political rights of demonstrators. For example, the confiscation of mobile phones or the siphoning of personal data by the authorities should be carried out only with the court's permission and under the supervision of an independent institution. In addition, a personal data protection authority must be established immediately to ensure adequate supervision. The personal data protection authority will oversee internet disconnection, content removal, and platform blocking policies. Without the supervision of an independent institution, police officers can take repressive actions arbitrarily under the pretext of maintaining public order.

CONCLUSION

Digital criminalisation can be prevented by reformulating articles in the ITE Law that are open to multiple interpretations. Criticism, satire, and suggestions must be treated as freedom of expression, not criminal offences. Strengthening the implementation of the PDP Law is essential to protect the political rights of demonstrators. In addition, a personal data protection authority must be established immediately to ensure adequate supervision. This reformulation is essential so that the ITE Law returns to its original purpose: protecting the public from cybercrime, not limiting freedom of expression. Legal norms in Indonesia are more defensive in their implementation, emphasising public order over people's fundamental rights. To address these weaknesses, Indonesia must adopt the GDPR principles and the Manila Principles on

Intermediary Liability to ensure more progressive digital rights protection. Indonesia also needs to establish an independent data protection authority and implement a court-approved mechanism for digital seizure and blocking.

REFERENCES

Aditya, N., & Akanksha. (2024). Digital media and its aspects. *Recent Researchers in Social Sciences and Humanities, 11*(1), 40–44. https://doi.org/10.5281/zenodo.11001492

Andersen, I. (2022). Well, that is just my opinion: The principle of expression and the public debate. *Journal of Deliberative Democracy, 18*(1). https://doi.org/10.16997/jdd.958

Asimah, D. (2020). To overcome the constraints of proof in the application of electronic evidence. *Jurnal Hukum Peratun, 3*(2), 97–110. https://doi.org/10.25216/peratun.322020.97-110

Budhijanto, D. (2024). *Revolusi cyberlaw Indonesia: Revisi UU ITE 2024, kedaulatan digital dan kecerdasan artifisial*. Refika Aditama.

Dirjosisworo, S. (2018). *Pengantar ilmu hukum* (19th ed.). Rajawali Pers.

Fadilah, K. (2025, September 9). Setelah 17+8 tuntutan rakyat dibawa ke Senayan. *DetikNews*. https://news.detik.com/berita/d-8097215/setelah-17-8-tuntutan-rakyat-dibawa-ke-senayan

Fitriansyah, D. R. (2025, September 15). Pembatasan internet, represi digital ala pemerintah. *Tempo*. https://www.tempo.co/infografik/infografik/pembatasan-internet-represi-digital-ala-pemerintah-2066684

Gea, A. Y. (2024). Development of criminal evidence law in Indonesia. *Legal Brief, 13*(3), 768–779. https://doi.org/10.35335/legal.v13i3.1031

Harahap, M. Y. (n.d.). *Pembahasan permasalahan dan penerapan KUHAP: Pemeriksaan sidang pengadilan, banding, kasasi, dan peninjauan kembali* (13th ed.). Sinar Grafika.

ISO/IEC. (2012). *ISO/IEC 27037:2012—Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*. https://amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

Kharismaningtyas. (2025, September 12). Kawal tuntutan rakyat 17+8: BEM UI soroti penahanan demonstran, Yusril temui Delpedro Marhaen. *Kompas TV*. https://www.kompas.tv/nasional/616715/kawal-tuntutan-rakyat-17-8-bem-ui-soroti-penahanan-demonstran-yusril-temui-delpedro-marhaen

Kurniawan, Y. S. (2019, September 15). Tindak pidana elektronik miskin solusi. *Hukum Online*. https://www.hukumonline.com/berita/a/tindak-pidana-elektronik-miskin-solusi-lt5d5e3d4e971fd/

Manila Principles. (n.d.). *Manila principles on intermediary liability*. https://manilaprinciples.org/

Mansyah, M. S., Suhartono, R. M., Salad, H., Dewi, R., & Bimasakti, D. H. (2023). Immunity rights of experts who provide statements in trials (Study Decision No. 47/Pdt.G/LH/2018/PN Cbi). *The Digest Journal of Jurisprudence and Legisprudence, 4*(2), 163–182.

Muhaimin. (2020). *Metode penelitian hukum*. Mataram University Press.

Mardianti, D. L. (2025, September 3). Kronologi demo memprotes DPR hingga meluas berubah penjarahan. *Tempo*. https://www.tempo.co/politik/kronologi-demo-memprotes-dpr-hingga-meluas-berubah-penjarahan-2065182

Negi, A., & Akanksha. (2024). Digital media and its aspects. *Recent Researchers in Social Sciences and Humanities, 11*(1), 40–44. https://doi.org/10.5281/zenodo.11001492

Prinst, D. (2022). *Hukum acara pidana dalam praktik*. Djambatan.

SAFEnet. (2025, September 13). Pernyataan sikap atas represi digital selama aksi Agustus 2025. https://safenet.or.id/id/2025/08/pernyataan-sikap-atas-represi-digital-selama-aksi-agustus-2025/

Siregar, R. A. (2025, September 8). Pengacara sebut aktivis Khariq Anhar yang ditahan Polda Metro dijerat UU ITE. *Detik*. https://www.detik.com/sumut/hukum-dan-kriminal/d-8096691/pengacara-sebut-aktivis-khariq-anhar-yang-ditahan-polda-metro-dijerat-uu-ite

Suryana, A., & Sakmaf, M. S. (2025). Can electronic evidence constitute sufficient grounds for criminal liability? *Jurnal Ilmu Hukum Kyadiren, 7*(1), 587–601. https://doi.org/10.46924/jihk.v7i1.323

Xiang, R. (2024). Enhancing democratic governance: The crucial role of broad public participation in government public consultations. *International Journal of Education and Humanities, 13*(3), 254–256. https://doi.org/10.54097/P8AQY810