



JiHK is licensed under Creative Commons Atribusi 4.0 Internasional license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



DOI: 10.46924/jihk.v8i2.518



Criminal Liability of Political Buzzers for Disseminating False Information on Social Media under Indonesia's 2026 Criminal Law Adjustments

James Simanjuntak^{1*}, Muhammad Rifky Adamsyah²

^{1,2} Institut Cinta Tanah Air, Indonesian

Correspondence

Muslim Lobubun, Institut Cinta Tanah Air Indonesia. JL. Petrus Kafiari Kel. Brambaken, Kec. Samofa, Kab. Biak Numfor, email:

jamesimanjuntak92@gmail.com

How to cite

Criminal Liability of Political Buzzers for Disseminating False Information on Social Media under Indonesia's 2026 Criminal Law Adjustments. (2026). *Jurnal Ilmu Hukum Kyadiren*, 8(2), 20-34.

<https://doi.org/10.46924/jihk.v8i2.518>

Original Article

Abstract

Political buzzers become a matter of criminal law when the amplification of political messages shifts into the dissemination of false news or notices through social media. This article examines the structure of the relevant offenses and the criminal liability of political buzzers after Indonesia's Criminal Code entered into force and was simultaneously adjusted by Law No. 1 of 2026 on Criminal Law Adjustments. Using prescriptive normative legal research, the study applies statutory, conceptual, and case approaches together with grammatical, systematic, teleological, and temporal interpretation. It finds that political buzzers do not constitute a special category of offender; liability turns on each person's conduct and culpability. For conduct committed before January 2, 2026, Article 28(3) in conjunction with Article 45A(3) of the EIT Law required intent, knowledge of falsity, electronic dissemination, and actual public unrest in physical space. Since January 2, 2026, Articles 263 and 264 of the Criminal Code, as adjusted by Law No. 1 of 2026, both require knowledge and actual public unrest, while differing in the type of prohibited content. Constitutional Court Decision No. 170/PUU-XXIV/2026 confirms their result-based character. The article proposes a six-layer test covering *tempus delicti* and *lex mitior*, attribution, content classification, *mens rea*, public unrest and causation, and modes of participation.

Keywords: criminal liability; political buzzers; false news; Criminal Law Adjustment Act; public unrest.

Abstrak

Fenomena buzzer politik menjadi persoalan hukum ketika amplifikasi pesan politik bergeser menjadi penyebaran berita atau pemberitahuan bohong melalui media sosial. Penelitian ini menganalisis konstruksi delik dan pertanggungjawaban pidana buzzer politik setelah KUHP Nasional berlaku dan disesuaikan melalui Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana. Penelitian menggunakan metode hukum normatif preskriptif dengan pendekatan perundang-undangan, konseptual, dan kasus serta penafsiran gramatikal, sistematis, teleologis, dan temporal. Hasil penelitian menunjukkan bahwa buzzer politik bukan subjek pidana khusus; pertanggungjawaban ditentukan oleh perbuatan dan kesalahan setiap orang. Untuk perbuatan sebelum 2 Januari 2026, Pasal 28 ayat (3) jo. Pasal 45A ayat (3) UU ITE mensyaratkan kesengajaan, pengetahuan atas kebohongan, penyebaran informasi elektronik, dan kerusahan nyata di ruang fisik. Sejak 2 Januari 2026, Pasal 263 dan Pasal 264 KUHP sebagaimana disesuaikan UU Nomor 1 Tahun 2026 sama-sama menuntut pengetahuan dan kerusahan aktual, dengan perbedaan pada kualifikasi konten. Putusan Mahkamah Konstitusi Nomor 170/PUU-XXIV/2026 mengeskakan karakter delik materiil tersebut. Artikel ini menawarkan uji enam lapis: *tempus delicti* dan *lex mitior*, atribusi akun/perbuatan, kualifikasi konten, *mens rea*, kerusahan dan kausalitas, serta penyertaan.

Kata kunci: pertanggungjawaban pidana; buzzer politik; berita bohong; UU Penyesuaian Pidana; kerusahan.

1. INTRODUCTION

Social media has transformed political communication from a largely one-way model into an almost continuous exchange of information. Digital platforms enable candidates, political parties, interest groups, volunteers, and ordinary citizens to communicate directly with the public while measuring responses in real time. At the same time, algorithmic systems tend to extend the reach of content that generates high levels of engagement. Within this environment, political buzzers operate to increase issue visibility, manufacture impressions of support, repeat selected narratives, or counter competing narratives. Studies of Indonesia's buzzer industry show that such activity is not merely spontaneous user expression; it may be organized through employment relations, divisions of labor, and particular political-economic interests.¹ More recent research likewise indicates that buzzers continue to shape public opinion during political contests on the X platform.²

The existence of political buzzers is not, in itself, a criminal-law problem. Posting expressions of support, crafting slogans, using hashtags, criticizing government policy, rebutting political opponents, or extending the reach of an opinion falls within the domain of political communication and is generally protected when undertaken lawfully. A legal problem arises when amplification networks are used to create or disseminate factual assertions known to be false and to direct them toward the public in a manner that satisfies the elements and consequences of a criminal offense. This boundary is crucial because digital space is also an arena for freedom of expression. Indonesia's experience with virtual democracy demonstrates that political debate on social media can readily develop into polarization and competing narratives, but those conditions cannot automatically be equated with criminal conduct.³

Distinguishing deliberately misleading content from information shared by mistake or in the reasonable belief that it is true is central to the assessment of culpability. Research on the resharing of hoaxes identifies significant variation in users' motives, acceptance, and awareness when forwarding information. From a criminal-law perspective, this variation means that the virality of a post cannot substitute for proof of the actor's state of mind. A user who knows that information is false and deliberately amplifies it is not situated in the same way as a user who reasonably believes the information to be accurate. Social categories such as buzzer, candidate supporter, volunteer, or political-account manager therefore cannot serve as shortcuts for inferring intent or knowledge.

Strict limits are especially important because false-information offenses in Indonesian cyber law have long presented interpretive difficulties. Scholarship on the enforcement of false-information provisions notes that uncertain boundaries between statutory elements can complicate application and produce divergent interpretations.⁴ From a criminal-law perspective, this variation means that the

¹ Shiddiq Sugiono, "Fenomena Industri Buzzer Di Indonesia: Sebuah Kajian Ekonomi Politik Media," *Communicatus: Jurnal Ilmu Komunikasi* 4, no. 1 (2020): 47–66, <https://doi.org/10.15575/cjik.v4i1.7250>.

² Novita Ika Purnamasari and Anjas Wijanarko, "Peran Buzzer Politik Ganjar-Mahfud Dalam Pembentukan Opini Publik Di Media Sosial X," *Warta ISKI* 7, no. 2 (2024): 146–59, <https://doi.org/10.25008/wartaiski.v7i2.290>.

³ Iswandi Syahputra, "Demokrasi Virtual Dan Perang Siber Di Media Sosial: Perspektif Netizen Indonesia," *Jurnal ASPIKOM* 3, no. 3 (2017): 457, <https://doi.org/10.24329/aspikom.v3i3.141>.

⁴ Melisa Arisanty et al., "Pengujian Konstruk Motif Sikap Penerimaan Dan Perilaku Membagikan Kembali Informasi Hoaks Dalam Media Sosial," *Jurnal Studi Komunikasi Dan Media* 25, no. 2 (2021): 171, <https://doi.org/10.31445/jskm.2021.4366>.

virality of a post cannot substitute for proof of the actor's state of mind. A user who knows that information is false and deliberately amplifies it is not situated in the same way as a user who reasonably believes the information to be accurate. Social categories such as buzzer, candidate supporter, volunteer, or political-account manager therefore cannot serve as shortcuts for inferring intent or knowledge.

Strict limits are especially important because false-information offenses in Indonesian cyber law have long presented interpretive difficulties. Scholarship on the enforcement of false-information provisions notes that uncertain boundaries between statutory elements can complicate application and produce divergent interpretations.⁵ Other research on Law No. 1 of 2024 identifies normative ambiguity and the potential chilling effect on freedom of expression as problems requiring greater precision in both statutory formulation and enforcement.⁶ The risk is heightened in political cases, where criticism, satire, propaganda, campaign claims, predictions, and factual assertions may all be delivered in equally brief and persuasive formats. Studies of criminalization risks under the EIT Law further underscore the need for disciplined interpretation so that legitimate criticism is not suppressed.⁷ The problem also relates to the broader need for regulatory convergence in technology law so that legal reform can respond to changing media and patterns of digital misconduct.⁸

Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) introduced a specific formulation governing the dissemination of false notices that cause public unrest. Article 28(3) prohibited any person from intentionally disseminating Electronic Information and/or Electronic Documents that the person knew contained a false notice causing public unrest, while Article 45A(3) prescribed the corresponding criminal sanction.⁹ The statutory structure therefore focuses not on the offender's social status or occupation, but on concrete conduct, knowledge of falsity, the use of electronic means, and the consequence specified by law.

The meaning of 'public unrest' was subsequently given a constitutional boundary by Constitutional Court Decision No. 115/PUU-XXII/2024. The Court held that public unrest must be understood as a condition disrupting public order in physical space, rather than mere commotion in digital or cyber space.¹⁰ Consequently, a trending topic, heated debate, a flood of comments,

⁵ Yenny Aman Serah et al., "Problematisasi Penegakan Hukum Perbuatan Menyebarkan Berita Bohong Dan Menyesatkan Terkait Pandemi Covid-19," *Jurnal IUS Kajian Hukum Dan Keadilan* 9, no. 2 (2021): 364–74, <https://doi.org/10.29303/ius.v9i2.878>.

⁶ M. Apandi et al., "Kekaburan Norma Dalam Kebebasan Berekspresi Di Era Digital: Analisis Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Hukum Lex Generalis* 5, no. 12 (2025), <https://doi.org/10.56370/jhlg.v5i12.1007>.

⁷ Abdurrahman Alhakim, "Urgensi Perlindungan Hukum Terhadap Jurnalis Dari Risiko Kriminalisasi UU Informasi Dan Transaksi Elektronik Di Indonesia," *Jurnal Pembangunan Hukum Indonesia* 4, no. 1 (2022): 89–106, <https://doi.org/10.14710/jphi.v4i1.89-106>.

⁸ Nurul Ula Ulya and Fazal Akmal Musyarri, "Omnibus Law Tentang Pengaturan Teknologi Informasi Dan Komunikasi Guna Rekonstruksi Konvergensi Hukum Teknologi," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 1 (2020): 53, <https://doi.org/10.33331/rechtsvinding.v9i1.399>.

⁹ Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. (2024) Pasal 28 ayat (3), Pasal 45A ayat (3), dan Pasal II angka 1.

¹⁰ Putusan Mahkamah Konstitusi Republik Indonesia Nomor 115/PUU-XXII/2024 Mengenai Pemaknaan "Kerusuhan" Sebagai Kondisi Yang Mengganggu Ketertiban Umum Di Ruang Fisik, Bukan Ruang Digital/Siber. (April 29, 2025).

coordinated attacks between accounts, or polarization of opinion does not automatically satisfy the consequence element. Article 28(3) required an actual disruption of public order and a provable causal connection between the false notice disseminated and the resulting unrest. This limitation is consistent with the constitutional requirement that cyber law not become an instrument of excessive criminalization.¹¹

Article 28(3) in conjunction with Article 45A(3) of the EIT Law must also be situated within its temporal framework. Article II(1) of Law No. 1 of 2024 provided that both provisions would remain in force only until Law No. 1 of 2023 on the Criminal Code took effect. Accordingly, for new conduct committed after January 2, 2026, substantive criminal liability can no longer be based on Article 28(3) in conjunction with Article 45A(3) of the EIT Law. The former provisions nevertheless remain relevant to conduct committed before that date, subject to the principle that a subsequent, more favorable criminal rule may apply to the accused.¹²

This transition was accompanied by a significant development that must be taken into account in legal analysis conducted in 2026. On January 2, 2026, simultaneously with the entry into force of the Criminal Code, Law No. 1 of 2026 on Criminal Law Adjustments also took effect.¹³ The new law amended Articles 263 and 264 of the Criminal Code.¹⁴ Article 263 now applies to a person who broadcasts or disseminates news or information that the person knows to be false and that causes public unrest. Article 264 addresses the dissemination of uncertain, exaggerated, or incomplete news that the person knows causes public unrest. The original formulations in Law No. 1 of 2023 using the standards of 'reasonably suspected' and 'may cause public unrest' therefore cannot be treated as a separate operative regime for new conduct committed after January 2, 2026.

The networked character of political buzzer activity adds a further layer of complexity. The persons who draft a narrative, control an account, upload content, coordinate amplification, pay for services, issue instructions, or provide the technical means may be different actors. Recent scholarship likewise emphasizes that political buzzer activity has not been established as a stand-alone offense and must therefore be assessed through the specific conduct, culpability, and statutory elements applicable to each actor. In these circumstances, imposing liability on an entire network solely because of political proximity or payment relationships would conflict with the principle of individualized criminal responsibility.¹⁵

Existing scholarship provides an important foundation on the buzzer industry, hoax-sharing behavior, ambiguity in the EIT Law, freedom of expression, and electronic evidence. The remaining research gap lies in integrating three legal developments that occurred in close succession: the end of

¹¹ Dona Budi Kharisma, "Kepatuhan Dan Kesadaran Hukum Kritis: Kajian Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 11, no. 1 (2022): 37, <https://doi.org/10.33331/rechtsvinding.v11i1.832>.

¹² Bagus Hermanto et al., "Dinamika Pengaturan Hukum Siber Indonesia: Refleksi Putusan Mahkamah Konstitusi Dalam Ius Constituendum," *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional* 14, no. 2 (2025), <https://doi.org/10.33331/rechtsvinding.v14i2.2045>.

¹³ Undang-Undang Nomor 1 Tahun 2026 Tentang Penyesuaian Pidana.

¹⁴ Pemerintah Republik Indonesia, *Undang Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana*, 2023.

¹⁵ Divello Pranaja and Dian Narwastuty, "Pertanggungjawaban Buzzer Terkait Penggiringan Opini Publik Berdasarkan Hukum Positif Indonesia," *As-Syar'i: Jurnal Bimbingan & Konseling Keluarga* 8, no. 2 (2026): 348–61, <https://doi.org/10.47467/as.v8i2.11121>; Mona Ervita and Ainun Jiwanti, "Perlindungan Pembela HAM-Lingkungan Dari Kriminalisasi Atas Tuduhan Konten Pencemaran Nama Baik Dan Berita Bohong: Perspektif Anti-SLAPP," *PUSKAPSI Law Review* 5, no. 2 (2025): 364–94, <https://doi.org/10.19184/puskapsi.v5i2.53781>.

Article 28(3) of the EIT Law as the substantive basis for new conduct; the immediate amendment of Articles 263 and 264 of the Criminal Code by Law No. 1 of 2026 on the very day the Criminal Code entered into force; and the reinforcement of the result-based character of those offenses through Constitutional Court Decision No. 170/PUU-XXIV/2026. This integration is particularly important when dissemination occurs through buzzer networks, because collective communication structures must not be converted into collective criminal liability.

Against this background, the article addresses two issues. First, it examines the structure of offenses involving the dissemination of false news or notices by political buzzers following the transition from the EIT Law to Articles 263 and 264 of the Criminal Code as adjusted by Law No. 1 of 2026. Second, it examines how individual liability and modes of participation may be established within buzzer networks without disregarding account attribution, *mens rea*, the consequence of physical public unrest, causation, and freedom of expression. The study's contribution lies in formulating a six-layer test tailored to the legal configuration actually in force since January 2, 2026, rather than to the original wording of the Criminal Code that was amended on the date it became effective.

2. RESEARCH METHODOLOGY

This study employs prescriptive normative legal research, treating law as a system of norms through which to assess the relationship among offense definitions, principles of criminal responsibility, modes of participation, electronic evidence, and the protection of freedom of expression. The study uses statutory, conceptual, and case approaches. Its principal primary legal materials include Law No. 1 of 2024, Law No. 1 of 2023, Law No. 1 of 2026 on Criminal Law Adjustments, Law No. 20 of 2025 on the Criminal Procedure Code, Constitutional Court Decision No. 115/PUU-XXII/2024, Constitutional Court Decision No. 170/PUU-XXIV/2026, and Supreme Court Circular Letter No. 1 of 2026. The constitutional framework is grounded in guarantees of freedom of expression, the right to obtain information, legal certainty, and statutory limitations on rights.

Secondary legal materials were selected primarily from accredited Indonesian journal articles addressing political buzzers, hoaxes, freedom of expression, cyber law, enforcement of the EIT Law, and digital criminal evidence. Communication scholarship was used to explain the structure and behavior of buzzer networks, while legal scholarship was used to assess the normative consequences of those structures. Sources were selected purposively according to their relevance to offense elements and criminal responsibility, with priority given to articles published in nationally accredited Sinta 1-Sinta 4 journals and to official primary sources so that legal developments after January 2, 2026 would not be obscured by literature published under the previous regime.

The analysis combines grammatical, systematic, and teleological interpretation with temporal analysis of the applicable norms. Grammatical interpretation distinguishes the meanings of 'disseminate,' 'broadcast,' 'distribute,' 'knows,' 'false,' 'uncertain,' 'exaggerated,' 'incomplete,' and 'causes public unrest.' Systematic interpretation connects substantive criminal provisions with the principle of legality, the application of more favorable subsequent law, rules on participation, and the new law of evidence. Teleological interpretation is used to assess the balance between protecting public order and preserving freedom of expression. Temporal analysis is indispensable because the wording of Articles

263 and 264 enacted in Law No. 1 of 2023 was amended by Law No. 1 of 2026 on the very date the Criminal Code entered into force.

The interpretive findings are synthesized into a six-layer analytical model. The model does not create new elements of criminal liability; rather, it establishes an order of analysis designed to prevent adjudicators from moving directly from the label 'buzzer' to a conclusion of guilt. The six layers are: *tempus delicti* and *lex mitior*; attribution of conduct and control of the account; content classification; *mens rea*; physical public unrest and causation; and the applicable mode of participation. Each layer is tied back to the statutory elements governing the time of the conduct, making the model a prescriptive tool for maintaining consistency among substantive criminal law, electronic evidence, and the principle of individualized responsibility.

3. RESULT AND DISCUSION

3.1. Structure of False-Information Offenses and the Temporal Scope of the EIT Law

The first finding is that 'political buzzer' is not a legal classification under the EIT Law, the Criminal Code, or the Criminal Law Adjustments Act. The statutory subject remains 'Every Person.' A person therefore cannot be convicted merely because the person works as a buzzer, is close to a political candidate, receives payment, or frequently posts political content. Such circumstances may provide context or evidentiary clues, but they do not replace the elements of the offense. The appropriate approach is functional: who did what, through which account or medium, in relation to what type of content, with what knowledge and intent, and whether the conduct actually caused the public unrest required by law.

For conduct committed while Article 28(3) in conjunction with Article 45A(3) of the EIT Law remained in force, at least five elements had to be read cumulatively: the subject 'Every Person'; the act of disseminating Electronic Information and/or Electronic Documents; intent; knowledge that the information contained a false notice; and the consequence of public unrest.¹⁶ Intent did not stand alone because the statutory language separately required knowledge of falsity. Proof that a person intentionally clicked an upload button was therefore insufficient unless it could also be shown that, at the relevant time, the person knew that the substance being disseminated was false.

The statutory concept of a 'false notice' should be treated more narrowly than the everyday concept of a hoax. Criminal law must distinguish factual assertions capable of being objectively verified from opinions, political judgments, satire, rhetorical hyperbole, predictions, or criticism. Scholarship on the enforcement difficulties surrounding false information shows that uncertainty as to the prohibited object can impede consistent application.¹⁷ Before examining an actor's political motive, law-enforcement authorities should therefore determine whether the content contains an objectively verifiable factual proposition and whether that proposition is demonstrably false. Unintentional factual errors, differences of interpretation, or statements that retain a factual basis should not be equated with information known to be false.

This classification becomes even more important in buzzer ecosystems, where content is often excerpted, retitled, combined with images, or reinforced through commentary. The assessment should not be confined to the final viral form of the content; it must also examine the relationship between the source material, the alterations made, and the representation presented to the public. If an actor receives an original document and then changes figures, removes a passage that reverses the meaning, or fabricates a

¹⁶ Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

¹⁷ Yenny Aman Serah et al., "Problematika Penegakan Hukum Perbuatan Menyebarkan Berita Bohong Dan Menyesatkan Terkait Pandemi Covid-19," *Jurnal IUS Kajian Hukum Dan Keadilan* 9, no. 2 (2021): 364–74, <https://doi.org/10.29303/ius.v9i2.878>.

quotation so that it appears to come from a particular source, that sequence of conduct may support an inference of knowledge. Conversely, not every edit or summary constitutes falsification. The criminal-law question remains whether the alteration produced a false factual assertion and whether the actor knew it was false.

Knowledge may be proven by direct evidence or inferred from a coherent chain of circumstances. In the digital context, an admission by the accused is not the only means of proof. Communications instructing participants to fabricate a false narrative, original and altered versions of a document, credible corrections received before reposting, or messages expressly stating an intention to mislead can support an inference of knowledge. Research showing differences between conscious acceptance of hoaxes and resharing based on a belief in their accuracy reinforces the need to avoid treating all disseminators alike.¹⁸ Political motive or payment may help explain why the conduct occurred, but neither substitutes for the knowledge required by the offense.

The most restrictive element of Article 28(3) was public unrest. The statutory explanation and Constitutional Court Decision No. 115/PUU-XXII/2024 located that consequence in a disruption of public order in physical space. Digital indicators such as views, reposts, comments, hashtags, or online disputes therefore cannot independently establish public unrest. Digital data may help demonstrate the reach of information and the process of mobilization, but the consequence required by the former provision remained an actual disturbance of public order. This interpretation preserves the distinction between political commotion as an ordinary feature of democracy and a condition that has crossed the threshold into disruption of public order.

Because public unrest is a consequence element, causation must also be proven. The fact that a post preceded unrest is only a starting point. Law-enforcement authorities must examine the relationship between the content of the false notice and the reasons for mass mobilization, the targeted audience, the intensity of dissemination, communications linking the content to conduct on the ground, and the presence or absence of other dominant causes. If clashes had already begun before the post appeared or were triggered by independent factors, it would be inappropriate to attribute the consequence solely because the content addressed the same issue. This causal approach is consistent with the result-based character of the offense emphasized by the Constitutional Court.

These limiting elements also have a constitutional dimension. Cybercrime law serves not only to protect society from information manipulation but also to prevent criminal provisions from being used to silence criticism. Research on the protection of environmental and human-rights defenders shows that allegations of defamation and false information can facilitate criminalization when offense elements are not applied rigorously.¹⁹ In the political arena, strict application strengthens rather than weakens the legitimacy of enforcement: genuinely false factual statements that satisfy the statutory consequence may be prosecuted, while opinions and criticism should not be drawn into the offense merely because they damage a particular actor's public image.

Temporal scope is the threshold issue in the analysis. Article II(1) of Law No. 1 of 2024 made Article 28(3) and Article 45A(3) transitional provisions that remained operative only until the Criminal Code took effect. The Criminal Code entered into force on January 2, 2026, and Law No. 1 of 2026 on Criminal Law Adjustments took effect on the same date. Article 28(3) in conjunction with Article 45A(3) therefore no longer provides the substantive basis for new conduct committed from that date onward. Conduct predating January 2, 2026 must nevertheless be assessed under the law in force when it occurred, while also applying rules governing subsequent legal changes that are more favorable to the accused.

For conduct committed on or after January 2, 2026, the appropriate reference points are Articles 263 and 264 of the Criminal Code as adjusted by Law No. 1 of 2026. Article 263 requires the broadcasting

¹⁸ Arisanty et al., "Pengujian Konstruksi Motif Sikap Penerimaan Dan Perilaku Membagikan Kembali Informasi Hoaks Dalam Media Sosial."

¹⁹ Mona Ervita and Ainun Jiwanti, "Perlindungan Pembela HAM-Lingkungan Dari Kriminalisasi Atas Tuduhan Konten Pencemaran Nama Baik Dan Berita Bohong: Perspektif Anti-SLAPP."

or dissemination of news or information known to be false and a resulting state of public unrest. Article 264 addresses a different category of content: uncertain, exaggerated, or incomplete news, with the requirement that the actor know that such news causes public unrest. The operative formulations no longer employ a 'reasonably suspected' standard and no longer use the phrase 'may cause public unrest.' The post-January 2, 2026 regime thus makes knowledge and an actual prohibited consequence the principal limits on criminalization.²⁰

These amendments change how cases involving buzzers must be structured. The principal distinction between Articles 263 and 264 now lies in the classification of the content, rather than in a gradation between knowledge and reasonable suspicion or between actual harm and potential danger. Article 263 applies to false news or information, whereas Article 264 covers news that is uncertain, exaggerated, or incomplete. Because both provisions require public unrest to have actually occurred, prosecutors cannot replace proof of that consequence with metrics of virality, comment volume, or the possibility of conflict. Content classification must come first, followed by proof of knowledge, consequence, and causation.

The phrase 'broadcast or disseminate' in the Criminal Code can encompass social-media conduct so long as the interpretation remains within the ordinary linguistic meaning of those terms. Uploading content to a public account, forwarding messages to a large group, or amplifying information through a network of accounts are all ways of making information available to others. Applying those terms to social media does not require the creation of a prohibited criminal-law analogy. It does, however, require proof of attribution: who actually controlled the account or device when the content was disseminated.

Conduct committed before January 2, 2026 but adjudicated after the Criminal Code entered into force requires application of the rules governing changes in criminal legislation. Article 3(1) of the Criminal Code generally directs courts to apply the new law unless the former provision is more favorable to the offender or aider. The comparison must address the legal configuration as a whole, including the conduct element, form of culpability, required consequence, penalty, and any circumstances affecting criminal liability. In this context, the relevant post-January 2, 2026 comparators are Articles 263 and 264 as adjusted by Law No. 1 of 2026, rather than the original formulations that had already been amended on the date the Criminal Code became effective.

Changes in substantive criminal law were accompanied by reform of criminal procedure. Law No. 20 of 2025 on the Criminal Procedure Code took effect on January 2, 2026 and expressly recognizes electronic evidence as a form of evidence. Article 235 also requires authentication and lawful acquisition. The EIT Law remains relevant to the concepts of Electronic Information and Electronic Documents and to the regulation of electronic systems, but the proof of contemporary criminal cases must now also be read together with the 2025 Criminal Procedure Code. Attribution of conduct to a buzzer should therefore be supported by account data, devices, metadata, electronic communications, and a chain of custody capable of demonstrating authenticity and lawful acquisition.²¹ The need to verify authenticity and harmonize the legal status of electronic evidence has likewise been emphasized in scholarship on electronic evidence in judicial proceedings.²²

The post-2026 framework received further constitutional reinforcement in Constitutional Court Decision No. 170/PUU-XXIV/2026. The Court rejected a request to add language that would, in substance, have permitted punishment based merely on the possibility that public unrest might arise. The reasoning confirms that the operative versions of Articles 263 and 264 remain result-based offenses: public

²⁰ Mona Ervita and Ainun Jiwanti, "Perlindungan Pembela HAM-Lingkungan Dari Kriminalisasi Atas Tuduhan Konten Pencemaran Nama Baik Dan Berita Bohong: Perspektif Anti-SLAPP."

²¹ Alfian Mardiansyah, "Mekanisme Pembuktian Dalam Perkara Tindak Pidana Siber (the Verification Mechanisms in the Event of Cyber Crime)," *Jurnal Legislasi Indonesia* 12, no. 4 (2008), <https://doi.org/10.54629/jli.v12i4.426>.

²² Pratama Herry Herlambang et al., "Harmonisasi Hukum UU Peratun Dan UU ITE Dalam Ketentuan Alat Bukti Elektronik Sebagai Alat Bukti Tambahan Dalam Sistem Peradilan Tata Usaha Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 1 (2024): 61–81, <https://doi.org/10.14710/jphi.v6i1.61-81>.

unrest must be proven as an actual consequence, not merely as an abstract risk. Public order is therefore protected through a defined threshold, while criticism, opinion, and digital debate cannot be transformed into criminal conduct without proof of the concrete consequence required by law.²³

3.2. Parameters for Controlling Discretion in the Designation of Certain Interests Based on the Social Function of Land and Agrarian Reform

Criminal liability for political buzzers must begin with the principle of individualized culpability. A network may explain how a narrative was designed and amplified, but criminal punishment remains personal and must be grounded in conduct and culpability that can be proven against a particular actor. Membership in a communication group, inclusion on a team list, or appearance within a payment network therefore does not automatically establish participation in a specific offense. The inquiry must focus on the actor's relevant contribution to the content at issue and the actor's state of mind regarding that content.

Attribution of an account is the first problem in individual liability. The registered account name, telephone number, or email address does not necessarily identify the person who made a particular post. Accounts may be jointly managed, delegated to administrators, accessed from different devices, or even used without authorization. Law-enforcement authorities should therefore connect the time of the post with login records, Internet Protocol addresses, devices, metadata, account-recovery history, electronic communications, and witness testimony. Electronic evidence should be evaluated as an internally corroborating chain rather than selected in isolation merely because it supports an initial suspicion.

Once conduct has been attributed, the inquiry turns to culpability. Under the former Article 28(3) regime, the EIT Law required both intentional dissemination and knowledge that the information contained a false notice. Under the regime in force since January 2, 2026, Articles 263 and 264 likewise retain knowledge as a central subjective element. Knowledge may be inferred, for example, when an actor participates in creating false information, receives authentic source material and then manipulates it, receives a credible correction but continues dissemination, or follows instructions that explicitly reveal fabrication. By contrast, payment, political alignment, and hashtag use may establish a relationship or motive, but they do not by themselves prove knowledge that particular content was false or otherwise fell within a prohibited category.

After the 2026 adjustment, the distinction between Articles 263 and 264 must be located primarily in the information itself. Article 263 requires proof that the news or information was false and that the actor knew it to be false. Article 264 does not require content to be wholly fabricated; it covers news that is uncertain, exaggerated, or incomplete. Neither provision, however, now permits criminal liability to be established through a 'reasonably suspected' standard. A failure to verify facts or a reasonable mistake therefore cannot automatically be converted into intent or knowledge. Prosecutors must identify concrete circumstances supporting a legally sound inference that the actor

²³ Pratama Herry Herlambang et al., "Harmonisasi Hukum UU Peratun Dan UU ITE Dalam Ketentuan Alat Bukti Elektronik Sebagai Alat Bukti Tambahan Dalam Sistem Peradilan Tata Usaha Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 1 (2024): 61–81, <https://doi.org/10.14710/jphi.v6i1.61-81>.

knew the character of the information disseminated and understood its connection to the prohibited consequence.

Liability within a buzzer network requires an analysis of modes of participation. Article 20 of the Criminal Code regulates principal offenders, including persons who commit an offense directly, act through an instrument or a person not criminally responsible, participate jointly, or induce another person through the means specified by law. Article 21 governs intentional assistance through the provision of opportunities, means, information, or other aid at the time the offense is committed. These provisions allow criminal law to reach actors operating behind public-facing accounts, but only when their contribution and intent satisfy the relevant mode of participation.

Within an organized network, several factual positions can be distinguished. First, a creator or editor who produces false content. Second, an account controller who performs the dissemination. Third, a coordinator who determines timing, targets, and amplification patterns. Fourth, a person who induces others by providing payment or other means. Fifth, a person who intentionally supplies access, devices, or information that facilitates the offense. Research on Indonesia's buzzer industry shows that divisions of labor and relationships among participants are characteristic features of organized buzzer operations. Such communicative roles, however, do not map automatically onto criminal-law categories of participation; each position must be tested against the applicable statutory requirements.

For example, a financier does not automatically become an instigator. If payment is made solely for lawful digital campaigning and the financier neither knows of nor intends the dissemination of falsehoods, participation cannot be established from the flow of funds alone. Conversely, where payment is tied to explicit instructions to fabricate false information, target a particular group, and coordinate dissemination, the evidence may support a theory of inducement or another form of participation. Research on buzzers and public-opinion formation shows that message coordination may be highly structured; what criminal law must additionally establish is the actor's purpose and contribution to the specific offense charged.

The same reasoning applies to secondary disseminators. A retweet, repost, or forwarded message is technically an act of dissemination, but culpability must still be proven. A user who shares content because the user believes it to be true cannot be treated in the same manner as a person who has been informed that the content is false and nevertheless continues to amplify it. Research on hoax-sharing behavior reinforces the importance of distinguishing users' motives, acceptance, and awareness. In network cases, this distinction prevents liability from expanding uncontrollably to thousands of users who merely interacted with the same content.

Consequence and causation must be incorporated into every theory of participation. Both former Article 28(3) of the EIT Law and Articles 263 and 264 after the 2026 adjustment require actual public unrest, not merely a potential for unrest. In a buzzer network, it is insufficient to prove that several accounts disseminated the same content. The prosecution must explain the relationship between the dissemination sequence and the disruption of public order in physical space, as well as how each actor's contribution fits the charged mode of participation. Participation doctrine cannot be used to eliminate the consequence element or conceal weaknesses in proving causation for the principal offense.

Electronic evidence is the principal means of mapping a buzzer network. Group communications may reveal instructions and divisions of responsibility; payment records may establish economic relationships; editorial files may show the origin and modification of a narrative; metadata and posting times may demonstrate coordination; and device or account-access data may connect an individual to specific conduct. Under the 2025 Criminal Procedure Code, electronic evidence is expressly recognized as evidence, but both authentication and lawful acquisition remain subject to scrutiny. A stand-alone screenshot should therefore not be treated as a shortcut where account attribution, conversational context, data integrity, or chain of custody remains contested.

On the basis of this analysis, the article proposes a six-layer test for the criminal liability of political buzzers. The first layer examines *tempus delicti* and *lex mitior* to determine the applicable law and whether a subsequent rule is more favorable to the accused. The second examines attribution of conduct and control of the relevant account. The third classifies the content, distinguishing false news or notices from opinion, criticism, and satire, and from uncertain, exaggerated, or incomplete news. The fourth examines *mens rea*, particularly the form of intent and knowledge required by the applicable provision.

The fifth layer examines physical public unrest and causation. Law-enforcement authorities must prove an actual disruption of public order in physical space and a sufficiently direct causal connection between the dissemination and that unrest. Virality, polarization, or digital commotion can provide contextual data but cannot substitute for the consequence element. The sixth layer examines the actor's role under the applicable rules of participation to determine whether the person acted as a direct perpetrator, indirect perpetrator, joint participant, instigator, or aider. These six layers do not create new statutory elements; they structure the order of analysis so that every conclusion of criminal liability can be traced back to valid law and admissible evidence.

The model helps avoid three analytical errors. The first is the status fallacy: treating the label 'buzzer' or the receipt of payment as proof of criminal culpability. The second is the virality fallacy: treating highly viral content as if it necessarily caused public unrest. The third is the network fallacy: attributing the same culpability to every member of a network. Each error shifts attention away from offense elements and toward social judgments about the actor. In criminal law, the complexity of a network increases, rather than reduces, the need to separate each participant's contribution, knowledge, and causal connection to the prohibited consequence.

Application of the model must distinguish between two legal periods. For conduct committed before January 2, 2026, law-enforcement authorities should assess Article 28(3) in conjunction with Article 45A(3) of the EIT Law in light of Constitutional Court Decision No. 115/PUU-XXII/2024 and the *lex mitior* principle where proceedings continue after the legal change. For conduct committed from January 2, 2026 onward, the applicable provision must be selected between Articles 263 and 264, as adjusted by Law No. 1 of 2026, according to the classification of the content, while knowledge, actual public unrest, and causation must still be proven. *Tempus delicti* therefore determines not merely the article number but the entire evidentiary structure of the case.

From the perspective of freedom of expression, the six-layer model provides a framework for proportionality. The 1945 Constitution guarantees freedom to express opinions and the right to communicate and obtain information, while permitting statutory restrictions necessary to respect the

rights of others and to meet legitimate demands of public order. Criticism of candidates, policy evaluation, political satire, or claims that remain within the realm of opinion should therefore be protected against overextension of criminal provisions. Scholarship on ambiguity in the EIT Law likewise emphasizes that clear boundaries are necessary to prevent a chilling effect on lawful expression. Recent research on digital democracy in Indonesia similarly identifies proportional enforcement and clear limits on expression as conditions for preserving freedom of speech on social media.

Protecting freedom of expression does not confer immunity for deliberate falsehoods. A clear separation between protected expression and criminal conduct enables the state to address information manipulation with greater legitimacy. Where the elements of an offense are satisfied, liability may extend to actors who design, control, induce, or assist dissemination according to their individual contributions and culpability. Conversely, where a case shows only criticism, opinion, satire, or digital commotion without the required physical public unrest, criminal proceedings should not be sustained by expanding the meaning of the offense. This limiting approach is consistent with the constitutional development of Indonesian cyber law and with the Constitutional Court's confirmation that Articles 263 and 264 are result-based offenses. The need for consistent interpretation and clear offense boundaries in EIT Law enforcement is also reflected in recent scholarship on online defamation after the 2024 reform.

The practical implication is the need for consistent case-handling guidance for investigators, prosecutors, and judges. Supreme Court Circular Letter No. 1 of 2026 provides general guidance on implementing the 2023 Criminal Code and the 2025 Criminal Procedure Code, but false-information cases involving digital networks still require a more specific analytical matrix. Each case file should ideally identify the *tempus delicti*, statutory basis, content category, evidence attributing the account, indicators of knowledge, the form of physical public unrest, the causal theory, and the mode of participation alleged against each actor. For digital evidence, documentation of authentication, lawful acquisition, and chain of custody should be assessed from the outset so that criminal liability does not rest solely on screenshots or account popularity.

Criminal liability can therefore reach the organizational structure of a political buzzer network without becoming collective liability. The law may reach persons who issue instructions or provide the means when evidence establishes their contribution and intent, while at the same time protecting persons whose relationship is merely political or social and who did not participate in the offense. This balance is essential if enforcement against false information is to protect public order without diminishing the quality of democratic discourse in digital space.

4. CONCLUSION

The criminal liability of political buzzers for disseminating false information is determined not by labels, occupation, political alignment, or receipt of payment, but by the conduct and culpability of each individual. The legal framework must be differentiated according to the time of the conduct. For conduct committed before January 2, 2026, Article 28(3) in conjunction with Article 45A(3) of the EIT Law required intent, knowledge that the information contained a false notice, dissemination

through electronic means, and actual public unrest in physical space. From January 2, 2026 onward, the substantive basis for new conduct shifted to Articles 263 and 264 of the Criminal Code as adjusted by Law No. 1 of 2026. Both operative provisions require knowledge and actual public unrest; their principal difference lies in the classification of the content. Constitutional Court Decision No. 170/PUU-XXIV/2026 reinforces their result-based character by rejecting an expansion that would have allowed the mere possibility of unrest to serve as a basis for criminal punishment.

Liability within buzzer networks must be established through individualized proof. This article formulates a six-layer test consisting of *tempus delicti* and *lex mitior*, attribution of conduct and account control, content classification, *mens rea*, physical public unrest and causation, and the applicable mode of participation. The model enables the law to reach narrative creators, account controllers, coordinators, instigators, and aiders where their contributions and culpability are proven, while preventing conviction based merely on status, virality, or network membership. Following the entry into force of the 2025 Criminal Procedure Code, electronic evidence must also satisfy requirements of authentication and lawful acquisition. Properly applied, this framework allows the law to target false information that genuinely satisfies the elements of a criminal offense without criminalizing legitimate criticism, opinion, satire, or political participation.

5. REFERENCES

Journals

- Alhakim, Abdurrahman. "Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia." *Jurnal Pembangunan Hukum Indonesia* 4, no. 1 (2022): 89–106. <https://doi.org/10.14710/jphi.v4i1.89-106>.
- Apandi, M., Karlina Rahayu, Wahyu Agus Prayugo, and Lisda Ariany. "Kekaburan Norma dalam Kebebasan Berekspresi di Era Digital: Analisis Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik." *Jurnal Hukum Lex Generalis* 5, no. 12 (2024). <https://doi.org/10.56370/jhlg.v5i12.1007>.
- Arisanty, Melisa, Gunawan Wiradharma, Yasir Riady, Sri Maulidia Permatasari, and Sri Sedyaningsih. "Pengujian Konstruksi Motif Sikap Penerimaan dan Perilaku Membagikan Kembali Informasi Hoaks dalam Media Sosial." *Jurnal Studi Komunikasi dan Media* 25, no. 2 (2021): 171–190. <https://doi.org/10.31445/jskm.2021.4366>.
- Ervita, Mona, and Ainun Jiwanti. "Perlindungan Pembela HAM-Lingkungan dari Kriminalisasi atas Tuduhan Konten Pencemaran Nama Baik dan Berita Bohong: Perspektif Anti-SLAPP." *PUSKAPSI Law Review* 5, no. 2 (2025): 364–394. <https://doi.org/10.19184/puskapsi.v5i2.53781>.
- Herlambang, Pratama Herry, Yos Johan Utama, and Aju Putrijanti. "Harmonisasi Hukum UU Peratun dan UU ITE dalam Ketentuan Alat Bukti Elektronik sebagai Alat Bukti Tambahan dalam

- Sistem Peradilan Tata Usaha Negara.” *Jurnal Pembangunan Hukum Indonesia* 6, no. 1 (2024): 61–81. <https://doi.org/10.14710/jphi.v6i1.61-81>.
- Hermanto, Bagus, Asrul Ibrahim Nur, and Indana Zulfa. “Dinamika Pengaturan Hukum Siber Indonesia: Refleksi Putusan Mahkamah Konstitusi dalam Ius Constituendum.” *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 14, no. 2 (2025): 315–335. <https://doi.org/10.33331/rechtsvinding.v14i2.2045>.
- Jorgi, Jhames, and Hery Firmansyah. “Digital Democracy and the Challenges of Freedom of Expression in Indonesia.” *Jurnal Ilmu Hukum Kyadiren* 8, no. 1 (2026): 293–308. <https://doi.org/10.46924/jihk.v8i1.476>.
- Kharisma, Dona Budi. “Kepatuhan dan Kesadaran Hukum Kritis: Kajian Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008.” *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 11, no. 1 (2022): 37–53. <https://doi.org/10.33331/rechtsvinding.v11i1.832>.
- Mardiansyah, Alfiyan. “Mekanisme Pembuktian dalam Perkara Tindak Pidana Siber (The Verification Mechanisms in the Event of Cyber Crime).” *Jurnal Legislasi Indonesia* 12, no. 4 (2015): 379–386. <https://doi.org/10.54629/jli.v12i4.426>.
- Pranaja, Divellio, and Dian Narwastuty. “Pertanggungjawaban Buzzer Terkait Penggiringan Opini Publik Berdasarkan Hukum Positif Indonesia.” *As-Syar’i: Jurnal Bimbingan & Konseling Keluarga* 8, no. 2 (2026): 348–361. <https://doi.org/10.47467/as.v8i2.11121>.
- Purnamasari, Novita Ika, and Anjas Wijanarko. “Peran Buzzer Politik Ganjar-Mahfud dalam Pembentukan Opini Publik di Media Sosial X.” *Warta ISKI* 7, no. 2 (2024): 146–159. <https://doi.org/10.25008/wartaiski.v7i2.290>.
- Serah, Yenny Aman, Anita Yulastini, and Rini Setiawati. “Problematisasi Penegakan Hukum Perbuatan Menyebarkan Berita Bohong dan Menyesatkan Terkait Pandemi Covid-19.” *Jurnal IUS Kajian Hukum dan Keadilan* 9, no. 2 (2021): 364–374. <https://doi.org/10.29303/ius.v9i2.878>.
- Sugiono, Shiddiq. “Fenomena Industri Buzzer di Indonesia: Sebuah Kajian Ekonomi Politik Media.” *Communicatus: Jurnal Ilmu Komunikasi* 4, no. 1 (2020): 47–66. <https://doi.org/10.15575/cjik.v4i1.7250>.
- Sutikni, Sutikni, Femmy Silaswaty, and Ida Aryati. “Legal Certainty in the Enforcement of Online Defamation Following the 2024 Reform of Indonesia’s Electronic Information and Transactions Law.” *Jurnal Ilmu Hukum Kyadiren* 8, no. 1 (2026): 660–674. <https://doi.org/10.46924/jihk.v8i1.491>.
- Syahputra, Iswandi. “Demokrasi Virtual dan Perang Siber di Media Sosial: Perspektif Netizen Indonesia.” *Jurnal ASPIKOM* 3, no. 3 (2017): 457–475. <https://doi.org/10.24329/aspikom.v3i3.141>.
- Ulya, Nurul Ula, and Fazal Akmal Musyarri. “Omnibus Law Tentang Pengaturan Teknologi Informasi dan Komunikasi Guna Rekonstruksi Konvergensi Hukum Teknologi.” *Jurnal Rechts Vinding:*

Media Pembinaan Hukum Nasional 9, no. 1 (2020): 53–70.
<https://doi.org/10.33331/rechtsvinding.v9i1.399>.

Legislation and Judicial Decisions

1945 Constitution of the Republic of Indonesia.

Law No. 1 of 2023 on the Criminal Code.

Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

Law No. 1 of 2026 on Criminal Law Adjustments.

Law No. 20 of 2025 on the Criminal Procedure Code.

Constitutional Court of the Republic of Indonesia, Decision No. 115/PUU-XXII/2024.

Constitutional Court of the Republic of Indonesia, Decision No. 170/PUU-XXIV/2026.

Supreme Court of the Republic of Indonesia, Circular Letter No. 1 of 2026 on Guidelines for Implementing the 2023 Criminal Code and the 2025 Criminal Procedure Code.