

Criminal Law Analysis of Discriminatory Content and Digital Radicalization on Online Platforms

Istiqlal Assaad

Universitas Muslim Indonesia Makassar

Received: November 17, 2025

Revised : December 10, 2025

Accepted: November 24, 2025

Published: December 24, 2025

Corresponding Author:

Author Name*: Istiqlal Assaad

Email*:

istiqlalassaad@umi.ac.id



Abstract: Digital platforms have become primary spaces for information dissemination while simultaneously facilitating the spread of discriminatory content and radicalization narratives that may threaten social order and national security. Within Indonesia's criminal law framework, the regulation of such phenomena remains problematic due to normative ambiguity, particularly in distinguishing the boundaries between freedom of expression, discriminatory speech, and radicalizing content. This study aims to analyze the regulation and application of criminal law concerning discriminatory and radical content on digital platforms and to examine the implications of normative ambiguity for legal certainty and human rights protection. Employing a normative juridical method with statutory, conceptual, and case approaches, the study finds that unclear definitions and regulatory overlap among the ITE Law, the Law on the Elimination of Racial and Ethnic Discrimination, and the Anti-Terrorism Law result in inconsistent law enforcement and the risk of over-criminalization. The study concludes that clearer and more harmonized criminal norms are essential to ensure legal certainty, effective enforcement, and the protection of human rights in the digital sphere.

Keywords: Criminal Law; Digital Radicalization; Discriminatory Content; Freedom of Expression; Legal Certainty

INTRODUCTION

The development of digital platforms has fundamentally transformed patterns of communication, the dissemination of information, and the formation of public opinion in society. Social media, online forums, and various content-based platforms have become primary spaces for individual expression as well as arenas for the exchange of ideas across geographic and social boundaries. However, behind their benefits as media for the democratization of information, digital spaces have also become fertile ground for the spread of discriminatory content, hate speech, and extreme ideological narratives that lead to processes of radicalization. This phenomenon indicates that digital transformation not only carries social and political implications, but also gives rise to

complex and multidimensional issues of criminal law.¹

From a juridical and sociological perspective, discriminatory content on digital platforms generally contains messages based on hatred, stereotypes, or stigma against certain groups based on race, ethnicity, religion, or other social identities. Such content not only has the potential to violate the right to equality and non-discrimination, but also often serves as an entry point for the dissemination of more extreme radicalization narratives. Indrianingsih and Budiarsih show that negative content on digital platforms has a

¹L. Indrianingsih & B. Budiarsih, "Analisis Hukum Konten Negatif di Platform YouTube di Indonesia," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, No. 3 (2022), <https://doi.org/10.53363/bureau.v2i3.71>

rapid and massive reach, so that its impact is no longer individual in nature, but collective and systemic.² In this context, digital space functions as an accelerator of social conflict and a threat to public order.

The characteristics of digital content dissemination that are rapid, cross-border, and difficult to control through conventional means pose serious challenges for criminal law enforcement. Unlike conventional crimes that are limited by space and time, digital content can be reproduced, modified, and disseminated instantly by multiple parties within a short period. Gamara and Ginting emphasize that this dynamic leads to an expansion of the meaning of criminal acts in cyberspace, including in the context of defamation, hate speech, and content containing elements of ethnicity, religion, race, and intergroup relations.³ This condition demands a criminal law framework that is capable of responding to technological developments without sacrificing the fundamental principles of the rule of law.

Within the Indonesian legal system, the dissemination of discriminatory content and radicalization narratives is regulated by various criminal law instruments. Law Number 19 of 2016 on Information and Electronic Transactions, particularly Article 28 paragraph (2), prohibits the dissemination of information intended to incite hatred or hostility based on ethnicity, religion, race, and intergroup

relations. In addition, Law Number 40 of 2008 on the Elimination of Racial and Ethnic Discrimination provides a criminal law basis for discriminatory acts, while Law Number 5 of 2018 on the Eradication of Terrorism Crimes regulates acts related to extreme ideology and radicalism. However, the existence of these various regulations does not automatically guarantee legal certainty in enforcement practice.⁴

The legal issue in this research is explicitly stated as the existence of normative ambiguity in Indonesian criminal law regarding the boundaries between freedom of expression, discriminatory speech, and content that leads to radicalization on digital platforms. This ambiguity is evident in the lack of clear normative definitions of “discriminatory content” and “radicalization”, as well as the overlap of regulation between the Law on Information and Electronic Transactions, the Law on the Elimination of Racial and Ethnic Discrimination, and the Law on Terrorism. As a result, the criminal parameters used in law enforcement become inconsistent and potentially give rise to violations of the principle of legality (*nullum crimen sine lege certa*).

From the perspective of criminal law, the principle of legality requires that an act may only be punished if it has been clearly and expressly formulated in statutory regulations. Unclear formulations of offenses have the potential to give rise to overly broad interpretations by law enforcement officials. Windisen and Adhari show that the application of Article 28 paragraph (2) of the Law on

²F. Gamara & R. Ginting, “Tindak Pidana Penghinaan sebagai Representasi Penyebarluasan Meme pada Platform Digital,” *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan* 10, no. 1 (2021), <https://doi.org/10.20961/recidive.v10i1.58844>

³UU No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

⁴Undang-Undang Nomor 40 Tahun 2008 tentang Penghapusan Diskriminasi Ras dan Etnis.

Information and Electronic Transactions in hate speech cases often depends on the subjective interpretation of law enforcement officials and judges, resulting in inconsistent decisions.⁵ This condition becomes even more problematic when discriminatory content is associated with processes of radicalization, because the standards of proof become more complex and sensitive to issues of national security.

On the other hand, criminal law must also take into account the protection of human rights, particularly freedom of expression. Articles 28D and 28I of the 1945 Constitution of the Republic of Indonesia guarantee equality before the law and protection from discrimination. However, restrictions on freedom of expression are permissible insofar as they are carried out proportionally and based on law. Hasibuan et al. emphasize that in the context of social media, restrictions on freedom of expression must be strictly tested so as not to turn into excessive criminalization of legitimate opinions.⁶ This tension between the protection of human rights and security interests constitutes an important normative background in the study of digital criminal law.

Normative ambiguity also affects the assessment of the element of fault (*mens rea*) in criminal acts involving the dissemination of digital content. Not all offensive or controversial content arises

from malicious intent to discriminate or radicalize. Kurniawati et al. emphasize that the identification of *mens rea* in the use of language in digital spaces requires an analysis of context, purpose, and the impact of the disseminated content.⁷ Without clear parameters, criminal law enforcement risks neglecting the principle of fault as the basis of criminal liability.

From an academic perspective, studies of digital criminal law in Indonesia still tend to be fragmented. Most research focuses on hate speech, pornography, or morality offenses on social media. Natasya and Andriasari, for example, examine law enforcement against revenge pornography based on the Law on Information and Electronic Transactions and the Pornography Law, while other studies highlight deepfakes or personal data protection.⁸ However, there is a lack of studies that link discriminatory content with processes of digital radicalization within a single comprehensive criminal law framework. In practice, discriminatory content often constitutes an initial stage that leads to the normalization of symbolic violence and extreme ideologies.

This academic gap indicates the need for a criminal law analysis that is not merely sectoral, but also integrative. Ayu emphasizes that the challenges of implementing the concept of the rule of law in the digital era require the renewal of criminal law approaches so that they are able to address digital crimes without

⁵W. Windisen & A. Adhari, "Penerapan Pasal 28 Ayat (2) UU ITE dalam Menanggulangi Delik Ujaran Kebencian di Internet," *Legal Standing: Jurnal Ilmu Hukum* 6, no. 1 (2021), <https://doi.org/10.24269/lj.v6i1.4292>

⁶K. Hasibuan, B. Aspani, & F. Fitriah, "Kebebasan Berpendapat dan Berekspres di Media Sosial Perspektif Hukum dan HAM," *Solusi* 22, no. 3 (2024), <https://doi.org/10.36546/solusi.v22i3.1335>

⁷R. Kurniawati, A. Aspani, & R. Marbun, "Identify *Mens Rea* in Language Use from a Criminal Law Perspective," *KnE Social Sciences* (2024), <https://doi.org/10.18502/kss.v8i21.14803>

⁸S. Natasya & D. Andriasari, "Penegakan Hukum terhadap Tindak Pidana Penyebaran Konten Pornografi Balas Dendam," *Bandung Conference Series: Law Studies* 3, no. 1 (2023), <https://doi.org/10.29313/bcsls.v3i1.4922>

sacrificing human rights principles.⁹ Accordingly, this research is not only normatively relevant, but also practically urgent to support consistency in the enforcement of digital criminal law.

Based on the foregoing, the novelty of this research lies in an integrative analysis of the dissemination of discriminatory content and digital radicalization within a single criminal law framework, with an emphasis on the problem of normative ambiguity and its implications for the principle of legality and the protection of human rights. This research aims to analyze the regulation and application of criminal law to the dissemination of discriminatory content and radicalization on digital platforms, as well as to examine the implications of normative ambiguity for legal certainty and the protection of human rights in the enforcement of digital criminal law.

METHDOLOGY

This research is a normative juridical legal study that focuses on the analysis of criminal law norms governing the dissemination of discriminatory content and radicalization on digital platforms. This method is chosen because the issues examined are directly related to the clarity of the formulation of criminal offenses, the principle of legality, and the consistency of regulation within statutory law.¹⁰ The approaches used include the statute approach, conceptual approach, and case approach. The statute approach is conducted by analyzing the 1945

Constitution of the Republic of Indonesia, the Criminal Code, Law Number 19 of 2016 on Information and Electronic Transactions, Law Number 40 of 2008 on the Elimination of Racial and Ethnic Discrimination, and Law Number 5 of 2018 on the Eradication of Terrorism Crimes. The conceptual approach is used to examine the concepts of discrimination, radicalization, hate speech, freedom of expression, and mens rea in criminal law. The case approach is carried out through an analysis of court decisions related to hate speech and digital radicalism cases.¹¹

This study employs a normative juridical method to examine the clarity and consistency of criminal law norms regulating discriminatory content and digital radicalization. Statutory, conceptual, and case approaches are used to identify normative ambiguity, interpret contested legal concepts, and assess inconsistencies in judicial application. Legal materials are analyzed using systematic and teleological interpretation to evaluate compliance with the principle of legality and human rights standards.

The legal materials used consist of primary legal materials in the form of statutory regulations and court decisions, secondary legal materials in the form of books and journal articles on criminal law and cyber law, and tertiary legal materials in the form of legal dictionaries and encyclopedias. All legal materials are analyzed in a normative-prescriptive manner using grammatical, systematic, and teleological interpretation to formulate recommendations for the renewal of digital criminal law norms that are more precise and proportional.

⁹R. Ayu, "Tantangan Penerapan Konsep Negara Hukum dalam Era Digital," *Jurnal Pengabdian Masyarakat dan Riset Pendidikan* 3, No. 4 (2025), <https://doi.org/10.31004/jerkin.v3i4.893>

¹⁰Sujadi, *Metode Penelitian Hukum* (Jakarta: Rajawali Press, 2012).

¹¹Ibid.

RESULT AND DISCUSSION

Normative Ambiguity of Criminal Law in the Regulation of Discriminatory Content and Digital Radicalization on Digital Platforms

Article 28(2) of the Law on Information and Electronic Transactions prohibits the dissemination of information intended to incite hatred or hostility, yet it fails to define the scope of ‘hatred’ and its distinction from radical ideological expression. This vagueness creates normative ambiguity, particularly when applied alongside the Law on the Elimination of Racial and Ethnic Discrimination, which regulates discrimination using different legal elements. The absence of clear differentiation between these norms undermines the *lex certa* principle and leads to inconsistent law enforcement.

The Law on Information and Electronic Transactions, particularly Article 28 paragraph (2), prohibits the dissemination of information that incites hatred or hostility based on ethnicity, religion, race, and intergroup relations, yet it does not provide a clear operational definition regarding the limits of “hatred”, “hostility”, nor their relationship with processes of radicalization. This lack of clarity creates broad interpretive space that potentially conflicts with the principle of legality, particularly the *lex certa* principle, which requires criminal offenses to be formulated clearly and without multiple interpretations.¹²

This ambiguity becomes more evident when Article 28 paragraph (2) of the Law on Information and Electronic Transactions is read in conjunction with

Law Number 40 of 2008 on the Elimination of Racial and Ethnic Discrimination. Law 40/2008 contains prohibitions on discriminatory acts with elements that differ relatively from the offense of hate speech under the Law on Information and Electronic Transactions. This overlap of norms raises juridical questions regarding the appropriate legal regime to prosecute certain acts in digital spaces, whether as cybercrime under the Law on Information and Electronic Transactions or as crimes of discrimination under Law 40/2008. Indrianingsih and Budiarsih show that overlapping regulation of negative content on digital platforms often results in inconsistent application of legal provisions by law enforcement authorities.¹³

On the other hand, the regulation of digital radicalization is often associated with Law Number 5 of 2018 on the Eradication of Terrorism Crimes. However, this law focuses on acts that have a direct relationship with terrorism offenses, while processes of digital radicalization often occur gradually through discriminatory narratives and the normalization of symbolic violence that do not necessarily meet the threshold of terrorism offenses. Kurniawan and Primawardani emphasize the importance of the principle of proportionality in restricting human rights in the context of terrorism in order to avoid excessive expansion of criminalization.¹⁴

Normative ambiguity is also reflected in the differences in standards of proof between hate speech and radical incitement. Hate speech is often treated as a formal offense, requiring only proof of the act of disseminating content, whereas

¹²UU No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

¹³L. Indrianingsih & B. Budiarsih, *op. cit.*

¹⁴A. Kurniawan & Y. Primawardani, “Proporsionalitas Pembatasan HAM dalam Pasal 28 UU Terorisme,” *Jurnal Legislasi Indonesia* 16, no. 1 (2019), <https://doi.org/10.54629/jli.v16i1.449>

radical incitement tends to be positioned as a material offense that requires proof of impact or a connection to subsequent crimes. This difference creates uncertainty in law enforcement practice, particularly when a single piece of digital content contains both discriminatory elements and extreme ideological narratives. Windisen and Adhari note that this inconsistency contributes to disparities in court decisions.¹⁵

The direct impact of such normative ambiguity is the threat to the principle of legality (*nullum crimen sine lege certa*). When the formulation of offenses lacks precision, law enforcement risks relying on extensive interpretation that may harm the rights of suspects and undermine legal certainty. Ayu emphasizes that the challenges faced by the rule of law in the digital era require precise formulation of criminal norms in order to prevent overcriminalization of legitimate expression.¹⁶ Therefore, the problem of normative ambiguity is not merely a technical legislative issue, but a fundamental issue of digital criminal law.

Criminal Liability for the Dissemination of Discriminatory Content and Digital Radicalization

Criminal liability in cases of dissemination of discriminatory content and digital radicalization involves complexity in terms of legal subjects and proof of fault. Legal subjects are not limited to individual content creators, but also include re-sharers and, under certain conditions, corporations or platform operators. Kanci et al. show that re-sharers of content containing criminal elements on social media may be held criminally liable if it is proven that they had awareness and intent to disseminate such content.¹⁷

¹⁵W. Windisen & A. Adhari, *op. cit.*

¹⁶R. Ayu, *op. cit.*

¹⁷H. Kanci, R. Leo, & H. Amalo, "Criminal Liability of Disseminators' Pornographic

The determination of *mens rea* becomes crucial in digital crimes. Not all dissemination of problematic content is carried out with malicious intent; some occur due to ignorance or negligence. Kurniawati et al. emphasize the importance of linguistic analysis and digital communication context to objectively identify the perpetrator's intent.¹⁸ Without clear parameters, law enforcement risks blurring the boundary between intent and negligence, which has implications for the fairness of sentencing. From the perspective of criminal offenses, the debate between formal offenses and material offenses becomes relevant. Article 28 paragraph (2) of the Law on Information and Electronic Transactions is often applied as a formal offense, while radicalization narratives linked to terrorism tend to require proof of consequences or causal connections. This difference creates evidentiary challenges, particularly in assessing the extent to which digital content contributes to processes of radicalization. Rais and Songkarn underline that cyber crimes affecting national security require careful standards of proof so as not to sacrifice due process of law.¹⁹

Evidentiary challenges become even more complex due to the nature of electronic evidence. The authenticity, integrity, and context of digital evidence must be ensured through reliable forensic procedures. Fernando et al. emphasize that the transformation of electronic evidence through digital forensics is an essential prerequisite for reforming criminal

Content on Social Media," *Journal of Digital Law and Policy* 2, no. 3 (2023), <https://doi.org/10.58982/jdlp.v2i3.384>

¹⁸R. Kurniawati et al., *op. cit.*

¹⁹M. Rais & P. Songkarn, "Hacker and the Threat for National Security," *Indonesian Journal of Counter Terrorism and National Security* 1, no. 1 (2022), <https://doi.org/10.15294/ijctns.v1i1.56728>

procedural law to ensure justice in cyber cases.²⁰ Without strong standards of proof, criminal liability risks becoming fragile and easily challenged in court.

To clarify the framework of criminal liability, the following analytical table is presented:

Table 1. Criminal Liability Framework for Discriminatory and Radical Content Online

Subject	Role in Dissemination	Mens Rea Requirement	Potential Liability
Content creator	Producing discriminatory/radical content	Intent or awareness	Principal offender
Re-sharer	Amplifying content	Knowledge and intent to disseminate	Accomplice/participant
Platform (corporate)	Hosting/moderation failure	Negligence or omission (conditional)	Corporate liability/administrative sanction

The table demonstrates that criminal liability is layered and contextual in nature. This approach is consistent with international practice that emphasizes human rights due diligence in content moderation. Nave and Lane emphasize that human rights due diligence obligations on digital platforms can function as a preventive mechanism without disproportionately expanding criminalization.²¹

Accordingly, criminal liability for the dissemination of discriminatory content and digital radicalization requires a balance between the effectiveness of law enforcement and the protection of human rights. Normative ambiguity and evidentiary challenges indicate the urgency

²⁰D. Fernando, D. Heniarti, & C. Zakaria, "Transformasi Alat Bukti Elektronik Menggunakan Digital Forensik," *Journal Justiciabelen* 5, no. 1 (2025), <https://doi.org/10.35194/jj.v5i01.5506>

²¹E. Nave & L. Lane, "Countering Online Hate Speech," *Computer Law & Security Review* 51 (2023), <https://doi.org/10.1016/j.clsr.2023.105884>

of refining a digital criminal law framework that is precise, proportionate, and oriented toward legal certainty.

Implications of Normative Ambiguity for the Protection of Human Rights and Legal Certainty in Digital Criminal Law Enforcement

Normative ambiguity in criminal law governing the dissemination of discriminatory content and digital radicalization carries serious implications for the protection of human rights and legal certainty in law enforcement practice. In a state governed by the rule of law, criminal law functions as an ultimatum remedium, to be applied only when other legal mechanisms are no longer adequate. However, when criminal norms are vague and open to multiple interpretations, criminal law risks becoming a repressive instrument that threatens freedom of expression and the principle of due process of law. This condition becomes increasingly critical in the digital sphere, where individual expression occurs on a massive and open scale.²²

One of the main implications of normative ambiguity is the risk of excessive criminalization of freedom of expression. Article 28 paragraph (2) of the Law on Information and Electronic Transactions is often applied without clear parameters distinguishing lawful expression from punishable speech. Hasibuan et al. emphasize that freedom of expression is a fundamental right that may only be restricted in a strict, proportionate manner and on the basis of clear law.²³ When criminal norms are not formulated with precision, law enforcement authorities tend to adopt an over-cautious approach that results in the criminalization of expression that should otherwise be protected.

²²K. Hasibuan et al., *op. cit.*

²³W. Windisen & A. Adhari, *op. cit.*

Normative ambiguity also contributes to inconsistencies in court decisions concerning digital content cases. In a number of cases, content with relatively similar characteristics has resulted in different judicial outcomes, depending on judges' interpretations of elements such as "hatred", "hostility", or "radicalism". Windisen and Adhari demonstrate that disparities in judicial decisions applying Article 28 paragraph (2) of the Law on Information and Electronic Transactions reflect the absence of binding interpretative guidelines.²⁴ Such inconsistency not only disadvantages defendants, but also undermines public trust in the criminal justice system.

Furthermore, normative ambiguity creates structural tension between national security interests and the protection of human rights. In the context of digital radicalization, the state has a legitimate interest in preventing the spread of extreme ideologies that may lead to terrorism. However, without clear normative boundaries, such preventive efforts risk violating the principle of proportionality. Kurniawan and Primawardani emphasize that restrictions on human rights based on national security must satisfy tests of legitimate aim, necessity, and balance.²⁵ When discriminatory content and radicalization are treated uniformly without normative differentiation, the space for civil liberties may be reduced in a disproportionate manner.

Another significant implication is legal uncertainty for law enforcement officials themselves. Normative ambiguity places authorities in a dilemma between their duty to enforce the law and the risk of violating human rights. In the absence of clear guidelines, law enforcement

processes become heavily dependent on individual discretion, which in turn increases the potential for abuse of power. Ayu emphasizes that the challenges faced by the rule of law in the digital era require normative clarity so that law enforcement officers do not act solely on the basis of subjective interpretation.²⁶

In the evidentiary context, normative ambiguity also complicates the application of fair standards of proof. Assessments of intent (*mens rea*) in the dissemination of digital content are often not accompanied by adequate contextual analysis. Kurniawati et al. emphasize that language in digital spaces is inherently multi-interpretable and highly contextual, requiring careful and evidence-based evaluation of the perpetrator's intent.²⁷ Without clear normative standards, the proof of *mens rea* risks being oversimplified, thereby undermining the principle of fault as the basis of criminal liability.

From an international perspective, the tendency to balance law enforcement with human rights protection is reflected in approaches based on human rights standards in content moderation. Oliva emphasizes that content moderation technologies must be subject to human rights principles, particularly freedom of expression and non-discrimination.⁷ This approach underscores the importance of normative clarity and accountability in any restriction of expression in digital spaces. In the Indonesian context, the absence of precise criminal parameters distances law

²⁴A. Kurniawan & Y. Primawardani, *op. cit.*

²⁵R. Ayu, *op. cit.*

²⁶T. Oliva, "Content Moderation Technologies," *Human Rights Law Review* 20 (2020): 607–640, <https://doi.org/10.1093/hrlr/ngaa032>

²⁷W. Ramirez & A. Siri, "Freedom of Speech and Its Digital Transformation," *Latin American Journal of European Studies* 5, no. 1 (2025), <https://doi.org/10.51799/2763-8685v5n1003>

enforcement practice from international human rights standards.

The urgency of reformulating digital criminal norms becomes increasingly evident when considering long-term impacts on democracy and the supremacy of law. Vague criminal norms not only harm individuals who come into conflict with the law, but also create a chilling effect that restricts public participation in digital discourse. Ramírez and Siri emphasize that the protection of freedom of expression in the digital era is a prerequisite for a healthy and inclusive democracy.⁸ Therefore, clarity and precision of criminal norms are essential conditions for ensuring a balance between security, public order, and human rights. Accordingly, normative ambiguity in criminal law governing discriminatory content and digital radicalization has systemic implications for the protection of human rights and legal certainty. Without precise and proportionate normative reformulation, digital criminal law enforcement risks losing its normative legitimacy and becoming a new source of injustice in the digital sphere.

CONCLUSION

The dissemination of discriminatory content and digital radicalization on digital platforms represents a complex and multidimensional criminal law issue with significant implications for social order and human rights protection. This study finds that normative ambiguity within the Law on Information and Electronic Transactions, the Law on the Elimination of Racial and Ethnic Discrimination, and their interaction with the Anti-Terrorism Law generates legal uncertainty and inconsistent enforcement of digital criminal law. Unclear boundaries between freedom of expression, discriminatory speech, and digital radicalization threaten the principle of legality and enable excessive criminalization.

Moreover, such ambiguity undermines freedom of expression and intensifies tensions between national security and the principle of proportionality. Accordingly, clearer criminal norms, regulatory harmonization, and human rights-based enforcement guidelines are necessary to ensure legal certainty, prevent abuse of authority, and uphold fair, proportionate, and legitimate digital criminal law within a democratic rule of law.

REFERENCE

Legal Document

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana (KUHP).

UU No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 40 Tahun 2008 tentang Penghapusan Diskriminasi Ras dan Etnis.

Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang.

Article

Ayu, R. (2025). Tantangan Penerapan Konsep Negara Hukum dalam Era Digital: Studi Kasus UU ITE dan Kebebasan Berekspresi. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*.

<https://doi.org/10.31004/jerkin.v3i4.893>.

Desita, A., Putri, A., Adelita, V., Gabrielle, M., Siregar, J., Kenotariatan, M., Hukum, F., & Airlangga, U. (2023). Community

- Criminal Responsibility For Dissemination Of News Containing Sara Through Social Media. *Santhet (Jurnal Sejarah Pendidikan Dan Humaniora)*.
<https://doi.org/10.36526/santhet.v7i2.3078>.
- Fernando, D., Heniarti, D., & Zakaria, C. (2025). Transformasi Alat Bukti Elektronik Menggunakan Digital Forensik Dalam Pembaharuan Hukum Acara Pidana. *Journal Justiciabelen (JJ)*.
<https://doi.org/10.35194/jj.v5i01.5506>.
- Gamara, F., & Ginting, R. (2021). Tindak Pidana Penghinaan Sebagai Representasi Penyebarluasan Meme Pada Platform Digital. *Recidive : Jurnal Hukum Pidana dan Penanggulangan Kejahatan*.
<https://doi.org/10.20961/recidive.v10i1.58844>.
- Hasibuan, K., Aspani, B., & Fitriah, F. (2024). Kebebasan Berpendapat Dan Berekspresi Di Media Sosial Prespektif Hukum Dan Hak Asasi Manusia. *Solusi*.
<https://doi.org/10.36546/solusi.v22i3.1335>.
- Indrianingsih, L., & Budiarsih, B. (2022). Analisis Hukum Konten Negatif Di Platform Youtube Di Indonesia. *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*.
<https://doi.org/10.53363/bureau.v2i3.71>.
- Kanci, H., Leo, R., & Amalo, H. (2023). Criminal Liability Of Disseminator's Pornographic Content On Social Media. *Journal of Digital Law and Policy*.
<https://doi.org/10.58982/jdlp.v2i3.384>.
- Kurniawan, A., & Primawardani, Y. (2019). Proporsionalitas Pembatasan Ham Dalam Pasal 28 Undang-Undang Pemberantasan Tindak Pidana Terorisme. *Jurnal Legislasi Indonesia*.
<https://doi.org/10.54629/jli.v16i1.449>.
- Kurniawati, R., , A., & Marbun, R. (2024). Identify Mens Rea in Language use from A Criminal Law Perspective. *KnE Social Sciences*.
<https://doi.org/10.18502/kss.v8i21.14803>.
- Maan, M., Amalo, H., & Dede, N. (2025). Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana. *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora*.
<https://doi.org/10.55606/jurrish.v4i1.5071>.
- Natasya, D., & Andriasari, D. (2023). Penegakan Hukum terhadap Tindak Pidana Penyebaran Konten Kejahatan Pornografi Balas Dendam (Revenge Porn) di Media Sosial Ditinjau dari UU ITE Dan UU Pornografi. *Bandung Conference Series: Law Studies*.
<https://doi.org/10.29313/bcsls.v3i1.4922>.
- Nave, E., & Lane, L. (2023). Countering online hate speech: How does human rights due diligence impact terms of service?. *Comput. Law Secur. Rev.*, 51, 105884.
<https://doi.org/10.1016/j.clsr.2023.105884>.
- Novera, O., & Fitri, Y. (2024). Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial. *El-Faqih : Jurnal Pemikiran dan Hukum*

- Islam.*
<https://doi.org/10.58401/faqih.v10i2.1539>.
- Oliva, T. (2020). Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression. *Human Rights Law Review*, 20, 607-640.
<https://doi.org/10.1093/hrlr/ngaa032>.
- Rais, M., & Songkarn, P. (2022). Hacker and the Treat for National Security: Challenges in Law Enforcement. *Indonesian Journal of Counter Terrorism and National Security*.
<https://doi.org/10.15294/ijctns.v1i1.56728>.
- Ramírez, W., & Siri, A. (2025). Freedom of Speech and Its Digital Transformation And Protection: guidelines and principles from the Inter-American Court Of Human Rights case-law and other human right protection bodies. *Latin American Journal of European Studies*.
<https://doi.org/10.51799/2763-8685v5n1003>.
- Siregar, G., & Sihite, I. (2020). Penegakan Hukum Pidana Bagi Pelaku Penyebar Konten Pornografi Di Media Sosial Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik. , 3, 1-11.
<https://doi.org/10.46930/jurnalrectum.v3i1.762>.
- Tiffani, S., & , F. (2024). Analisis Hukum Terhadap Perlindungan Data Pribadi (Studi Kasus @farida.nurhan dan @codebluuuu). *Jurnal Ilmu Hukum, Humaniora dan Politik*.
<https://doi.org/10.38035/jihhp.v4i3.1915>.
- Windisen, W., & Adhari, A. (2021). Penerapan Pasal 28 Ayat (2) Undang-

Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dalam Menanggulangi Delik Ujaran Kebencian Di Internet. *Legal Standing : Jurnal Ilmu Hukum*.
<https://doi.org/10.24269/lis.v6i1.4292>.

Book

Sujadi. *Metode Penelitian Hukum*. Jakarta: Rajawali Press, 2012