PATTIMURA Law Study Review

Volume 3 Nomor 3 Desember, 2025: h. 254 - 260
E-ISSN: 3025-2245
: 10.47268/palasrev.v3i3.24004

Kriminalisasi *Cyber-Retribution* (Pembalasan Digital) dan Fenomena *Digital Mob Justice*: Komparasi Batasan Hukum Pidana Indonesia dan Korea Selatan dalam Melindungi *Privacy Interest*

Rahmalina Nurul Mudyawati[1*], Melani Nurul Mudyawati[2]

[1,2] Fakultas Syariah dan Hukum Universitas Islam Negeri Sunan Gunung Djati, Bandung, Indonesia.

: rahmalinanm@gmail.com

ABSTRACT: *This study is motivated by the escalating phenomenon of cyber-retribution and digital mob justice, which poses a significant threat to individual privacy rights. The objective of this research is to analyze the comparative criminal law boundaries between Indonesia and South Korea regarding digital retribution and the protection of privacy interests. This research employs a normative legal method with statutory and comparative approaches. The findings reveal that Indonesian criminal law remains fragmentary, relying heavily on ambiguous defamation offenses under the Electronic Information and Transactions (ITE) Law, thus failing to protect privacy comprehensively. Conversely, South Korea demonstrates a more progressive legal framework with specific regulations explicitly targeting doxing and non-consensual content dissemination. In conclusion, Indonesia requires a reconstruction of cybercrime offenses to shift the legal paradigm from merely protecting reputation to safeguarding substantial privacy interests.*

Keywords: Cyber-Retribution; Digital Mob Justice; Privacy Interest; Comparative Criminal Law.

ABSTRAK: Penelitian ini dilatarbelakangi oleh maraknya fenomena cyber-retribution dan digital mob justice yang mengancam hak privasi individu. Tujuan penelitian ini adalah menganalisis perbandingan batasan hukum pidana antara Indonesia dan Korea Selatan dalam merespons pembalasan digital serta perlindungan privacy interest. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan komparatif. Hasil penelitian menunjukkan bahwa hukum pidana Indonesia masih bersifat fragmentaris dan cenderung bergantung pada delik pencemaran nama baik dalam UU ITE yang multitafsir, sehingga gagal melindungi privasi secara komprehensif. Sebaliknya, Korea Selatan telah memiliki regulasi yang lebih spesifik dan progresif dalam menjangkau tindakan doxing serta penyebaran konten non-konsensual. Kesimpulannya, Indonesia perlu merekonstruksi delik kejahatan siber agar bergeser dari paradigma perlindungan kehormatan semata menuju perlindungan privacy interest yang substansial.

Kata Kunci: Cyber-Retribution; Digital Mob Justice; Kepentingan Privasi; Hukum Pidana Komparatif.

PENDAHULUAN

Erupsi teknologi digital yang terintegrasi secara mendalam ke dalam tatanan sosial telah mengubah lanskap viktimisasi modern, melahirkan varian kriminalitas baru yang mengeksploitasi data pribadi sebagai senjata. Di tengah konvergensi ini, dua fenomena kriminologi spesifik muncul sebagai ancaman serius terhadap integritas individu: *Cyber-Retribution* dan *Digital Mob Justice*. *Cyber-Retribution* bermanifestasi sebagai tindakan pembalasan berbasis digital, seringkali melalui penyebaran konten intim non-konsensual (*Non-Consensual Intimate Imagery*) atau *doxing*, yang bertujuan untuk menghancurkan reputasi korban secara permanen di ruang publik.[1] Sementara itu, *Digital Mob Justice* merepresentasikan pergeseran mekanisme kontrol sosial, di mana massa warganet

[1] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Cambridge: Harvard University Press, 2014), h. 56.

mengambil alih fungsi peradilan dengan melakukan penghakiman kolektif dan persekusi daring terhadap individu yang dianggap melanggar norma, sering kali dengan mengabaikan asas praduga tak bersalah.[2] Kedua fenomena ini tidak hanya menciptakan kerugian psikologis dan sosial yang ireversibel, tetapi juga secara fundamental menantang doktrin perlindungan *privacy interest* (kepentingan privasi) dalam hukum pidana konvensional yang sering kali gagap merespons kecepatan dan luasnya jangkauan serangan digital tersebut.

Kendati diskursus mengenai kejahatan siber telah berkembang, tinjauan literatur terkini menunjukkan adanya lakuna yang signifikan dalam analisis komparatif yang mendalam. Sebagian besar penelitian yang ada cenderung terfragmentasi; studi di Indonesia umumnya terpaku pada kritik normatif terhadap ambiguitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tanpa menawarkan perspektif perbandingan global yang memadai.[3] Di sisi lain, literatur internasional yang membahas Korea Selatan sering kali berfokus secara eksklusif pada dampak sosiologis dari kasus profil tinggi seperti "Nth Room" tanpa mengelaborasi bagaimana konstruksi hukum mereka dapat diadopsi oleh negara berkembang.[4] Ketiadaan studi yang secara holistik menyandingkan batasan kriminalisasi (*criminalization limits*) antara Indonesia dan Korea Selatan menciptakan kekosongan pengetahuan, padahal Korea Selatan menawarkan model yurisdiksi yang sangat relevan mengingat kemajuan infrastruktur digital mereka yang berbanding lurus dengan tingginya tingkat litigasi *cyber-defamation* dan kejahatan seksual digital. Oleh karena itu, urgensi untuk membedah bagaimana kedua negara menyeimbangkan perlindungan privasi dengan kebebasan berekspresi menjadi sangat krusial untuk mencegah normalisasi anarki di ruang siber.

Berangkat dari kesenjangan teoretis dan praktis tersebut, penelitian ini bertujuan untuk menjawab pertanyaan mendasar: bagaimana hukum pidana Indonesia dan Korea Selatan membatasi dan mendefinisikan tindak pidana *cyber-retribution* serta *digital mob justice* dalam kerangka perlindungan *privacy interest*? Penelitian ini secara spesifik bertujuan untuk menganalisis secara komparatif efektivitas rezim hukum di kedua negara dalam menanggulangi pembalasan digital, serta mengevaluasi apakah pendekatan represif yang diterapkan Korea Selatan dapat menjadi rujukan bagi reformasi hukum di Indonesia. Analisis ini tidak hanya akan menyoroti persamaan dan perbedaan dalam elemen delik pidana, tetapi juga akan mengukur sejauh mana instrumen hukum yang ada mampu memberikan pemulihan (*remedy*) yang adil bagi korban yang privasinya telah dilanggar secara masif oleh tindakan massa digital.

Kebaruan (*novelty*) dari kajian ini terletak pada pendekatan komparatif spesifik yang membedah irisan antara "pembalasan pribadi" dan "penghakiman massa" di ranah digital, sebuah area yang jarang dieksplorasi dalam satu kerangka analisis hukum pidana terpadu. Berbeda dengan penelitian sebelumnya yang parsial, studi ini menawarkan kontribusi orisinil berupa evaluasi kritis terhadap batas toleransi hukum (*legal tolerance*) terhadap *vigilantism* digital di dua sistem hukum Asia yang berbeda karakter namun menghadapi tantangan demografi digital yang serupa. Identifikasi masalah dan tujuan penelitian ini menjadi sangat penting mengingat absennya regulasi yang adaptif dapat berujung pada delegitimasi sistem peradilan formal. Sistematika penulisan artikel ini akan diawali dengan analisis kerangka hukum positif di kedua negara, dilanjutkan dengan studi perbandingan

[2] Daniel Trottier, "Digital Vigilantism as Weaponisation of Visibility," *Philosophy & Technology* 30, no. 1 (2017): 55–72

[3] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber* (Bandung: Refika Aditama, 2012), h. 45–48

[4] J. Kim and S. Lee, "The Nth Room Case and the Evolution of Digital Sex Crimes in South Korea," *Asian Journal of Criminology* 16, no. 3 (2021): 203–218.

kasus konkret, dan diakhiri dengan sintesis rekomendasi kebijakan hukum pidana (*criminal policy*) yang responsif untuk memperkuat perlindungan privasi di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan paradigma Yuridis Normatif (Doctrinal Research), berfokus pada analisis kaidah dan norma hukum positif dalam merespons fenomena *Cyber-Retribution* dan *Digital Mob Justice*. Pendekatan utama yang digunakan adalah Pendekatan Perundang-undangan (*Statute Approach*) dan Pendekatan Komparatif (*Comparative Approach*). Data penelitian berupa Data Sekunder, yang mencakup Bahan Hukum Primer (Undang-Undang ITE, UU PDP, KUHP Indonesia, serta *Act on Promotion of Information and Communications Network Utilization and Information Protection* Korea Selatan) dan Bahan Hukum Sekunder (jurnal ilmiah terkini, buku, dan laporan resmi). Pengumpulan data dilakukan melalui Studi Kepustakaan (*Library Research*) dengan mengidentifikasi, mengklasifikasi, dan mengkompilasi regulasi serta putusan yurisprudensi dari kedua yurisdiksi. Teknik analisis data yang digunakan adalah Analisis Kualitatif dengan menerapkan Teknik Komparasi Fungsional (*Functional Comparative Method*). Analisis ini melibatkan dua tahap: pertama, Interpretasi Hukum (gramatikal dan teleologis) untuk memahami konstruksi delik dan unsur *mens rea* yang terkait dengan *doxing* dan *cyber-retribution* di kedua negara. Kedua, Perbandingan Fungsional yang bertujuan membandingkan *ratio legis* dan batasan kriminalisasi yang diterapkan oleh Indonesia dan Korea Selatan dalam mengatasi masalah sosial yang sama (pelanggaran privasi masif). Hasil komparasi ini kemudian disintesiskan untuk merumuskan rekomendasi kebijakan hukum pidana (*criminal policy*) yang bersifat preskriptif guna memperkuat perlindungan *privacy interest* di Indonesia.

HASIL DAN PEMBAHASAN

Bab ini menyajikan analisis mendalam mengenai konstruksi hukum pidana di Indonesia dan Korea Selatan dalam merespons fenomena *Cyber-Retribution* dan *Digital Mob Justice*. Pembahasan difokuskan pada evaluasi kritis terhadap batasan kriminalisasi (*criminalization limits*) dan efektivitas norma hukum dalam melindungi kepentingan privasi (*privacy interest*). Uraian ini sekaligus mengelaborasi kesenjangan teoretis yang telah dipaparkan pada bagian pendahuluan, dengan menyoroti bagaimana perbedaan paradigma hukum di kedua negara menghasilkan tingkat perlindungan yang asimetris bagi korban.

A. Analisis Kriminalisasi *Cyber-Retribution* dan *Digital Mob Justice* di Indonesia: Hegemoni Moralitas di Atas Privasi

1. Identifikasi Norma dan Ambiguitas Definisi dalam Rezim Hukum Siber

Temuan penelitian menunjukkan bahwa rezim hukum pidana Indonesia, yang utamanya disangga oleh Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), masih mengadopsi pendekatan yang sangat "berorientasi pada konten" (*content-oriented*) daripada "berorientasi pada persetujuan" (*consent-oriented*).

Cyber-Retribution yang bermanifestasi sebagai penyebaran konten intim non-konsensual (*Non-Consensual Intimate Imagery*/NCII), Pasal 27 ayat (1) UU ITE menjadi instrumen utama. Namun, analisis gramatikal terhadap pasal ini mengungkapkan kelemahan fundamental: frasa "melanggar kesusilaan" menitikberatkan pada sifat asusila dari konten tersebut, bukan

pada ketiadaan izin (konsen) dari subjek data atau niat jahat (*mens rea*) pelaku untuk melakukan pembalasan.[5] Hal ini menciptakan ambiguitas hukum di mana korban yang konten pribadinya disebar sebagai bentuk balas dendam justru berpotensi turut dikriminalisasi sebagai partisipan dalam pembuatan konten asusila. Teori viktimologi modern menyebut kondisi ini sebagai *secondary victimization* oleh negara, di mana hukum gagal membedakan antara pelaku kejahatan kesusilaan dengan korban eksploitasi seksual.[6]

Meskipun Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS) telah mencoba mengisi kekosongan ini dengan memperkenalkan Pasal 14 mengenai kekerasan seksual berbasis elektronik, harmonisasi dengan UU ITE masih menyisakan celah implementatif. Unsur "pembalasan" (*retribution*) belum diakui secara eksplisit sebagai elemen pemberat pidana yang berdiri sendiri dalam UU ITE.[7] Akibatnya, hukum gagal menangkap esensi *Cyber-Retribution* sebagai kejahatan terhadap otonomi tubuh dan privasi, melainkan mereduksinya sekadar menjadi gangguan terhadap ketertiban umum dan moralitas publik.[8]

2. Keterbatasan Yuridis dalam Menjangkau Fenomena *Digital Mob Justice*

Terkait fenomena *Digital Mob Justice*—di mana massa digital melakukan persekusi melalui *doxing*—analisis yuridis menunjukkan adanya kevakuman norma yang signifikan. Indonesia belum memiliki regulasi yang secara spesifik mengkriminalisasi mobilisasi massa digital untuk tujuan penghakiman main hakim sendiri. Upaya penegakan hukum saat ini terpaksa menggunakan pasal umum seperti pencemaran nama baik (Pasal 27A UU ITE) atau pengancaman (Pasal 29 UU ITE). Pendekatan ini memiliki dua kelemahan fatal: 1) Isu Subjektivitas: Delik pencemaran nama baik mensyaratkan adanya unsur "menyerang kehormatan" yang bersifat subjektif. Dalam kasus *doxing* yang dilakukan oleh *Digital Mob Justice*, pelaku sering kali berlindung di balik dalih "kebenaran" atau *public interest defense* untuk mengungkap kejahatan orang lain, sehingga sulit dijerat pidana;[9] 2) Absennya Pertanggungjawaban Kolektif: Hukum pidana Indonesia menganut asas *individual liability*. Struktur ini menyulitkan aparat penegak hukum untuk menjerat ribuan akun anonim yang berpartisipasi dalam persekusi digital (*piling on*). Undang-Undang Perlindungan Data Pribadi (UU PDP) Pasal 67 ayat (2) memang memidana pengungkapan data pribadi, namun sanksi pidananya belum teruji efektif dalam menghadapi fenomena viralitas massa yang masif dan terdesentralisasi.[10] Temuan ini mengonfirmasi kritik dalam *state of the art* sebelumnya bahwa regulasi Indonesia cenderung reaktif dan parsial, gagal melihat *Digital Mob Justice* sebagai bentuk viktimisasi sistematis yang memerlukan pendekatan pidana khusus di luar delik penghinaan konvensional.[11]

B. Paradigma Progresif Korea Selatan: Proteksi Privasi dan Pencegahan *Retribution*

1. Spesifikasi Delik dan Perluasan Cakupan Kriminalisasi

Berbeda dengan pendekatan Indonesia yang masih berkutat pada definisi kesusilaan, Korea Selatan telah mengembangkan kerangka hukum yang sangat spesifik dan responsif terhadap evolusi kejahatan digital. Melalui *Act on Special Cases Concerning the Punishment,*

---

[5] Ari Wibowo, "Kebijakan Kriminalisasi Penyebaran Konten Intim Non-Konsensual," *Jurnal Mimbar Hukum* 32, no. 3 (2020), h. 452.

[6] Sinta Dewi Rosadi, *Hukum Perlindungan Privasi dan Data Pribadi di Era Ekonomi Digital* (Bandung: Alumni, 2021), h. 88.

[7] Dwi Suryahartanto Putra, "Analisis Yuridis Pasal Kesusilaan dalam UU ITE Pasca Revisi," *Jurnal Rechts Vinding* 10, no. 1 (2021), h. 60.

[8] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber* (Bandung: Refika Aditama, 2018), h. 112.

[9] Indah Permatasari and Topo Santoso, "Doxing dan Tantangan Penegakan Hukum Pidana di Indonesia," *Padjadjaran Jurnal Ilmu Hukum* 8, no. 2 (2021), h. 195.

[10] Hari Sutra Disemadi, *Hukum Siber Indonesia: Tantangan dan Perspektif Masa Depan* (Jakarta: Rajawali Pers, 2022), h. 145.

[11] Daniel Trottier, "Digital Vigilantism as Weaponisation of Visibility," *Philosophy & Technology* 30, no. 1 (2017), h. 58.

etc. of Sexual Crimes, Korea Selatan tidak hanya mengkriminalisasi distribusi NCII, tetapi juga secara eksplisit memperberat hukuman jika tindakan tersebut dilakukan dengan tujuan pembalasan atau ancaman (*threat to distribute*).[12]

Analisis terhadap legislasi Korea pasca kasus "Nth Room" menunjukkan adanya pergeseran paradigma dari "perlindungan moralitas" menuju "perlindungan integritas korban". Legislatif Korea merevisi undang-undang untuk memperluas definisi pelaku, tidak hanya mencakup pembuat dan penyebar konten, tetapi juga mereka yang memiliki atau menonton konten eksploitasi seksual yang dihasilkan dari paksaan.[13] Hal ini memutus rantai permintaan (*demand*) dalam ekosistem *Cyber-Retribution*, sebuah langkah progresif yang belum diadopsi dalam hukum positif Indonesia.

2. Kriminalisasi *Doxing* dan *Cyber Defamation* Berbasis Fakta

Konteks *Digital Mob Justice*, Korea Selatan menerapkan batasan hukum yang jauh lebih ketat melalui *Act on Promotion of Information and Communications Network Utilization and Information Protection* (Network Act). Poin krusial yang membedakannya dengan Indonesia adalah kriminalisasi terhadap Cyber Defamation yang berbasis fakta (Article 70). Hukum Korea Selatan memidana seseorang yang menyebarkan fakta (kebenaran) melalui jaringan informasi jika dilakukan dengan *tujuan khusus* (*purpose*) untuk memfitnah atau merusak reputasi seseorang.[14] Ketentuan ini sangat efektif meredam *Digital Mob Justice* dan *doxing*, karena para pelaku persekusi digital tidak dapat berlindung di balik argumen bahwa data yang mereka sebar adalah fakta. Hal ini menegaskan teori bahwa dalam yurisdiksi Korea, *privacy interest* dan hak untuk dilupakan (*right to be forgotten*) ditempatkan pada hierarki yang setara atau bahkan lebih tinggi dibandingkan kebebasan berekspresi yang tidak bertanggung jawab.[15]

C. Komparasi Kritis: Menuju Rekonstruksi Perlindungan *Privacy Interest*

1. Divergensi Filosofis dan Konsekuensi Penegakan Hukum

Membandingkan temuan di kedua negara, terlihat jelas adanya divergensi filosofis. Indonesia memandang *Cyber-Retribution* melalui kacamata moralitas publik, di mana negara bertindak sebagai penjaga kesusilaan. Sebaliknya, Korea Selatan memandangnya melalui kacamata privasi dan keamanan individu, di mana negara bertindak sebagai pelindung otonomi warga negara.

Konsekuensi dari perbedaan ini sangat nyata. Di Indonesia, korban *Cyber-Retribution* sering kali enggan melapor karena takut dikriminalisasi balik atau dipermalukan secara prosedural.[16] Di Korea Selatan, kerangka hukum yang ada memberikan insentif bagi korban untuk melapor karena adanya jaminan perlindungan identitas dan mekanisme penghapusan konten yang terintegrasi dengan sistem peradilan pidana, seperti mandat penghapusan konten oleh *Digital Sex Crime Victim Support Center* yang didukung undang-undang.[17]

---

[12] *Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes*, Act No. 17264, May 19, 2020, art. 14 (South Korea).

[13] Jiyoung Kim and Sookyoung Lee, "The Nth Room Case and the Evolution of Digital Sex Crimes in South Korea," *Asian Journal of Criminology* 16, no. 3 (2021), h. 205.

[14] J. Yun, "Cyber Defamation and the 'Truth' Defense in South Korean Law," *Journal of Korean Law* 18, no. 2 (2019), h. 30.

[15] S. Choi and M. Kim, "Victimization and Legal Protection in Cyberspace: A Comparative Analysis of South Korea and the United States," *International Journal of Law, Crime and Justice* 62 (2020), h. 108.

[16] Harkristuti Harkrisnowo, "Rekonstruksi Hukum Pidana Indonesia dalam Menghadapi Kejahatan Digital," *Jurnal Hukum Pidana dan Kriminologi* 2, no. 1 (2021), h. 15.

[17] Jung-In Lee, "Legal Responses to Digital Sex Crimes in South Korea: Focus on the Nth Room Case," *Pacific Rim Law & Policy Journal* 30, no. 2 (2021), h. 260.

2. Mengisi Kekosongan Hukum Indonesia

Mengacu pada teori perlindungan data sebagai hak asasi yang fundamental, temuan ini menunjukkan bahwa Indonesia perlu segera mereformasi batasan hukum pidananya. Ketiadaan delik yang spesifik mengatur "niat pembalasan" (*retaliatory intent*) dan ambiguitas dalam penanganan *mob justice* merupakan kelemahan struktural.[18] Indonesia perlu mengadopsi pendekatan Korea Selatan dalam memisahkan elemen "konten asusila" dengan "konten non-konsensual", serta mempertimbangkan kriminalisasi *doxing* yang bersifat jahat (*malicious doxing*) tanpa bergantung pada unsur pencemaran nama baik semata. Tanpa reformasi ini, *privacy interest* di Indonesia akan terus tergerus oleh anarki digital yang berlindung di balik kekosongan norma hukum.[19]

KESIMPULAN

Berdasarkan pembahasan dan analisis yang telah diuraikan pada bab-bab sebelumnya, penelitian ini menarik tiga simpulan utama sebagai jawaban atas permasalahan hukum yang diajukan. Pertama, konstruksi hukum pidana Indonesia saat ini dalam merespons fenomena *Cyber-Retribution* dan *Digital Mob Justice* masih bersifat fragmentaris dan tidak memadai. Pengaturan yang ada cenderung bergantung pada delik pencemaran nama baik dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang bersifat multitafsir. Pendekatan ini terbukti gagal dalam memberikan perlindungan spesifik terhadap *privacy interest*, karena titik berat pemidanaan masih diletakkan pada aspek serangan terhadap kehormatan, bukan pada pelanggaran privasi itu sendiri. Kedua, sebaliknya, Korea Selatan telah menunjukkan paradigma hukum yang jauh lebih progresif melalui pemberlakuan regulasi khusus, seperti *Act on Punishment of Digital Sex Crimes*. Hukum positif Korea Selatan secara eksplisit mengkriminalisasi tindakan penyebaran konten non-konsensual dan praktik *doxing* dengan standar pembuktian yang terukur serta sanksi pidana yang berat, sehingga memberikan kepastian hukum yang konkret bagi korban kekerasan digital. Sintesis perbandingan antara kedua negara menunjukkan adanya divergensi fundamental pada *ratio legis* atau landasan filosofis perlindungan hukum. Indonesia masih terpaku pada perlindungan "nama baik" (*honor/reputation*) di mana privasi sering kali dikaburkan dengan ketertiban umum atau moralitas publik. Sementara itu, Korea Selatan telah menempatkan "integritas privasi" (*privacy integrity*) sebagai hak dasar yang otonom dan tidak dapat dilanggar (*inviolable rights*). Perbedaan orientasi ini menyebabkan penegakan hukum di Indonesia sering kali terjebak pada ambiguitas pasal karet, sedangkan Korea Selatan mampu menjangkau esensi kerugian korban akibat *digital vigilantism* secara lebih presisi. Sebagai rekomendasi *ius constituendum*, Indonesia perlu segera melakukan reformulasi kebijakan kriminal dengan bergeser dari paradigma perlindungan reputasi menuju perlindungan privasi yang substantif. Pembentuk undang-undang disarankan untuk menyusun regulasi spesifik atau merevisi KUHP dan UU ITE dengan mengadopsi unsur-unsur pelindungan privasi ala Korea Selatan, khususnya dalam mengkriminalisasi *doxing* dan penyebaran data pribadi untuk tujuan pembalasan (*retribution*). Hal ini diperlukan agar hukum pidana tidak lagi menjadi alat yang multitafsir, melainkan instrumen yang efektif dalam melindungi hak privasi warga negara di era digital.

[18] Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik* (Jakarta: Rajawali Pers, 2019), h. 90.
[19] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Cambridge: Harvard University Press, 2014), h. 56.

REFERENSI

Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes, Act No. 17264, May 19, 2020, art. 14 (South Korea).

Ari Wibowo, "Kebijakan Kriminalisasi Penyebaran Konten Intim Non-Konsensual," *Jurnal Mimbar Hukum* 32, no. 3 (2020).

Danielle Keats Citron, *Hate Crimes in Cyberspace*, Cambridge: Harvard University Press, 2014.

Daniel Trottier, "Digital Vigilantism as Weaponisation of Visibility," *Philosophy & Technology* 30, no. 1 (2017): 55–72.

Dwi Suryahartanto Putra, "Analisis Yuridis Pasal Kesusilaan dalam UU ITE Pasca Revisi," *Jurnal Rechts Vinding* 10, no. 1 (2021).

Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Jakarta: Rajawali Pers, 2019.

Hari Sutra Disemadi, *Hukum Siber Indonesia: Tantangan dan Perspektif Masa Depan*, Jakarta: Rajawali Pers, 2022.

Harkristuti Harkrisnowo, "Rekonstruksi Hukum Pidana Indonesia dalam Menghadapi Kejahatan Digital," *Jurnal Hukum Pidana dan Kriminologi* 2, no. 1 (2021).

Indah Permatasari and Topo Santoso, "Doxing dan Tantangan Penegakan Hukum Pidana di Indonesia," *Padjadjaran Jurnal Ilmu Hukum* 8, no. 2 (2021).

J. Kim and S. Lee, "The Nth Room Case and the Evolution of Digital Sex Crimes in South Korea," *Asian Journal of Criminology* 16, no. 3 (2021): 203–218.

J. Yun, "Cyber Defamation and the 'Truth' Defense in South Korean Law," *Journal of Korean Law* 18, no. 2 (2019).

Jiyoung Kim and Sookyoung Lee, "The Nth Room Case and the Evolution of Digital Sex Crimes in South Korea," *Asian Journal of Criminology* 16, no. 3 (2021).

Jung-In Lee, "Legal Responses to Digital Sex Crimes in South Korea: Focus on the Nth Room Case," *Pacific Rim Law & Policy Journal* 30, no. 2 (2021).

S. Choi and M. Kim, "Victimization and Legal Protection in Cyberspace: A Comparative Analysis of South Korea and the United States," *International Journal of Law, Crime and Justice* 62 (2020).

Sigid Suseno, *Yurisdiksi Tindak Pidana Siber* (Bandung: Refika Aditama, 2018.

Sinta Dewi Rosadi, *Hukum Perlindungan Privasi dan Data Pribadi di Era Ekonomi Digital*, Bandung: Alumni, 2021.