

DOXING SEBAGAI KEJAHATAN SIBER: STUDI KOMPARATIF ANTARA INDONESIA DAN SINGAPURA

Ranisa Diati¹, Irwan Triadi²

¹Magister Hukum, Fakultas Hukum, Universitas Pembangunan Nasional Veteran Jakarta

² Fakultas Hukum, Universitas Pembangunan Nasional Veteran Jakarta

Corresponding Author: Ranisa Diati

Email: diatiranisa@gmail.com

Abstract

The development of digital technology has given rise to new forms of crime that have not been fully anticipated by traditional legal systems. One increasingly prevalent phenomenon is the practice of doxing, which is the act of disclosing and disseminating someone's personal information without permission for a specific purpose, often to harass, intimidate, or harm the victim. The purpose of this study is to analyze doxing as a form of cybercrime from the perspective of Indonesian and Singaporean law. In Indonesia, regulations regarding doxing have not been specifically regulated, but can only be prosecuted through Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, and Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). In contrast, Singapore has been more progressive by explicitly prohibiting doxing through the Protection from Harassment Act (POHA) of 2014, which was later updated. The normative-comparative legal research method compares the legal constructions of Indonesia and Singapore in addressing doxing and examines the urgency of establishing specific regulations in Indonesia. The research findings indicate that Indonesia's regulations remain general and do not provide adequate legal certainty, while Singapore has succeeded in providing more concrete legal protections for doxing victims. The researchers recommend that Indonesia immediately formulate specific regulations regarding doxing, either through a revision of the UU ITE or the creation of a new law on cybercrime.

Keywords: *doxing; cybercrime; UU ITE; POHA.*

Abstrak

Perkembangan teknologi digital telah melahirkan bentuk-bentuk kejahatan baru yang belum sepenuhnya diantisipasi oleh sistem hukum tradisional. Salah satu fenomena yang semakin marak adalah praktik *doxing*, yaitu tindakan mengungkapkan dan menyebarkan informasi pribadi seseorang tanpa izin dengan maksud tertentu, sering kali untuk melecehkan, mengintimidasi, atau membahayakan korban. Adapun tujuannya untuk menganalisis *doxing* sebagai bentuk kejahatan siber dalam perspektif hukum Indonesia dan Singapura. Di Indonesia, regulasi mengenai *doxing* belum diatur secara spesifik, melainkan hanya dapat dijerat melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sebaliknya, Singapura telah lebih progresif dengan mengatur secara eksplisit larangan *doxing* melalui *Protection from Harassment Act (POHA)* tahun 2014 yang kemudian diperbarui. Metode penelitian hukum normatif-komparatif, dengan membandingkan konstruksi hukum Indonesia dan Singapura dalam menangani *doxing*, serta mengkaji urgensi pembentukan peraturan khusus di Indonesia. Hasil penelitian menunjukkan bahwa pengaturan Indonesia masih bersifat umum dan tidak memberikan kepastian hukum yang memadai, sementara Singapura berhasil menghadirkan perlindungan hukum yang lebih konkret terhadap korban *doxing*. Peneliti merekomendasikan agar Indonesia segera merumuskan regulasi khusus mengenai *doxing*, baik melalui revisi UU ITE maupun pembentukan undang-undang baru tentang kejahatan siber.

Kata Kunci: *doxing; kejahatan siber; UU ITE; POHA*

1. Pendahuluan

Perkembangan teknologi informasi telah memberikan kontribusi besar terhadap kehidupan manusia. Era digital memfasilitasi komunikasi, pendidikan, transaksi ekonomi, bahkan pemerintahan secara lebih cepat dan efisien¹. Namun, bersamaan dengan itu, muncul pula ancaman baru berupa tindak pidana siber yang terus berkembang seiring kemajuan teknologi. Salah satu bentuk kejahatan siber yang belakangan mendapat perhatian serius adalah praktik *doxing*². Istilah *doxing* berasal dari kata documents atau docs yang kemudian dipendekkan menjadi *dox* dengan imbuhan *-ing*. Secara sederhana, *doxing* berarti tindakan mengumpulkan dan menyebarkan informasi pribadi seseorang, seperti alamat rumah, nomor telepon, akun media sosial, hingga data pekerjaan, tanpa izin dari orang yang bersangkutan, dengan maksud tertentu yang biasanya merugikan korban³. Praktik ini sering kali dilakukan melalui media sosial atau platform digital lain, dan dampaknya bisa sangat serius, mulai dari gangguan privasi hingga ancaman keselamatan jiwa.

Di Indonesia, fenomena *doxing* semakin marak dalam beberapa tahun terakhir. Kasus-kasus penyebaran data pribadi pejabat publik, tokoh politik, hingga selebriti di media sosial menjadi perhatian masyarakat luas. Misalnya, kasus penyebaran data pribadi salah satu pejabat publik yang kemudian memicu ancaman serta serangan digital dari pihak-pihak tertentu. Namun, meskipun praktik ini semakin sering terjadi, sistem hukum Indonesia belum memiliki aturan khusus yang secara tegas mengatur tindak pidana *doxing*.

Regulasi yang ada baru terbatas pada Undang-Undang Nomor 11 Tahun 2008

tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)⁴. Kedua undang-undang ini memberikan perlindungan terhadap data pribadi dan melarang penyalahgunaannya. Namun, karena tidak secara eksplisit menyebut istilah "*doxing*," maka penegakan hukum masih menghadapi berbagai kendala, baik dari segi pembuktian maupun kepastian hukum.⁵

Sebaliknya, Singapura menjadi salah satu negara di Asia Tenggara yang cukup progresif dalam merespons fenomena ini. Melalui *Protection from Harassment Act* (POHA) yang diundangkan pada tahun 2014 dan diperbarui pada tahun 2019, Singapura secara eksplisit mengatur mengenai tindak pidana *doxing*. POHA memberikan perlindungan yang komprehensif bagi korban pelecehan dan ancaman digital, termasuk tindakan pengungkapan data pribadi secara tidak sah.

Sebagai bukti nyata pelaksanaan POHA di Singapura, dalam debat anggaran tahun 2021 disebutkan bahwa sejak UU tersebut mulai berlaku pada 15 November 2014, telah diajukan 853 aplikasi untuk *Protection Orders* kepada pengadilan termasuk kasus pelecehan seksual, pelecehan di tempat kerja, pelecehan daring, dan pelecehan antara tetangga. Dari jumlah tersebut, 348 di antaranya dikabulkan, sementara 366 *Expedited Protection Orders* (EPO) diberikan sebagai tindakan sementara untuk melindungi pemohon sebelum sidang utama. Secara khusus untuk *doxing*, hingga 31 Desember 2020 terdapat 29 kasus *doxing* yang diajukan ke State Courts di Singapura setelah

¹ Ernani Yunita, Maeda Istiza, and Apriliantoni, "Pentingnya Teknologi Informasi Dan Komunikasi Dalam Sehari-Hari," *El-Idare: Journal of Islamic Education Management* 11, no. 1 (2025): 134–40, <http://jurnal.radenfatah.ac.id/index.php/El-idare>.

² David M. Douglas, "Doxing: A Conceptual Analysis," *Ethics and Information Technology* 18, no. 3 (2016): 199–210, <https://doi.org/10.1007/s10676-016-9406-0>.

³ *Ibid.*

⁴ M Faza and R Wiyanti, "Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah," *Jurnal Hukum Siber* 9, no. 1 (2024): 45–60.

⁵ Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58".

amandemen POHA tahun 2019 yang menjadikannya tindak pidana⁶.

POHA (Amandemen 2019) juga memperluas definisi “*identity information*” atau informasi identitas yang dilindungi tidak hanya nama dan alamat rumah, tetapi termasuk alamat email, nomor telepon, tanggal lahir, alamat pekerjaan, foto atau video, dan informasi tentang keluarga atau pendidikan korban⁷. Selain itu, amandemen ini memperkenalkan *Protection from Harassment Court* (PHC), sebuah pengadilan khusus yang mulai beroperasi pada 1 Juni 2021 untuk menangani secara terpadu seluruh kasus-kasus berkaitan dengan POHA, dengan prosedur disederhanakan dan timeline yang dipercepat untuk kasus-kasus tertentu⁸.

Dengan demikian, Singapura telah memiliki dasar hukum yang jelas untuk menindak pelaku *doxing*⁹. Berdasarkan latar belakang tersebut, tulisan ini bertujuan untuk menganalisis perbandingan pengaturan hukum mengenai *doxing* di Indonesia dan Singapura, sekaligus mengkaji urgensi pembentukan regulasi khusus di Indonesia.

2. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perbandingan hukum Indonesia dan Singapura. Sumber data utama berupa peraturan perundang-undangan, literatur hukum, jurnal akademik, dan putusan pengadilan terkait. Pendekatan yang digunakan meliputi; pendekatan perundang-undangan (*statute approach*) dengan mengkaji UU ITE, UU PDP di Indonesia, serta POHA di Singapura, pendekatan konseptual (*conceptual approach*) dengan mengkaji teori privasi,

perlindungan data pribadi, dan kejahatan siber, pendekatan komparatif (*comparative approach*) dengan membandingkan konstruksi hukum di Indonesia dan Singapura.

3. Hasil dan Pembahasan

Konsep *Doxing* sebagai Kejahatan Siber

Doxing dikategorikan sebagai kejahatan siber karena dilakukan melalui sarana elektronik dan memiliki dampak terhadap hak privasi seseorang. Menurut penelitian internasional, *doxing* memiliki tiga elemen pokok: (1) adanya pengumpulan data pribadi; (2) adanya penyebaran data tanpa izin; dan (3) adanya maksud merugikan atau menimbulkan ancaman bagi korban¹⁰.

Dalam perspektif hukum pidana, *doxing* dapat dikualifikasikan sebagai tindak pidana karena melanggar hak dasar individu atas privasi. Privasi sendiri telah diakui sebagai bagian dari hak asasi manusia sebagaimana tertuang dalam Pasal 28G ayat (1) UUD 1945 yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya¹¹.

Pengaturan *doxing* di Indonesia, belum ada ketentuan hukum yang secara eksplisit mengatur tentang *doxing*. Namun, terdapat beberapa pasal yang dapat digunakan untuk menjerat pelaku, antara lain:

a. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE):

- 1) Pasal 26 ayat (1) mengatur bahwa penggunaan informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan dengan persetujuan yang bersangkutan.

⁶ Fabiah Koh, “Budget Debate: 853 Applications for Protection Orders Made since Introduction of Anti-Harassment Law in November 2014,” *The Straits Times*, 2021, <https://www.straitstimes.com/singapore/politics/budget-debate-853-applications-for-protection-orders-made-since-introduction-of>

⁷ Laney Zhang, “Singapore: Amendment to Harassment Law Passed to Criminalize ‘Doxing’.”

2019, <https://www.loc.gov/item/global-legal-monitor/2019-10-25/singapore-amendment-to-harassment-law-passed-to-criminalize-doxing/>.

⁸ “Ministry of Law Singapore, ‘Commencement of Protection from Harassment Court on 1 June 2021’, Press Release.”

⁹ Ministry of Law Singapore, ‘Amendments to the Protection from Harassment Act (POHA),’ 2019.

¹⁰ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).

¹¹ Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G.

- 2) Pasal 27 ayat (3) melarang distribusi atau akses terhadap informasi elektronik yang bermuatan penghinaan atau pencemaran nama baik.
 - 3) Pasal 28 ayat (2) melarang penyebaran informasi untuk menimbulkan kebencian atau permusuhan antarindividu atau kelompok.¹²
- b. Undang-Undang Perlindungan Data Pribadi (UU PDP):
- 1) UU No. 27 Tahun 2022 memberikan definisi dan perlindungan terhadap data pribadi, termasuk hak subjek data.
 - 2) Pasal 65 sampai Pasal 70 UU PDP mengatur sanksi pidana terhadap pelanggaran pengolahan data pribadi tanpa hak.

Meskipun demikian, kekurangan mendasar dalam sistem hukum Indonesia adalah belum adanya istilah "*doxing*" secara eksplisit, sehingga menimbulkan ketidakpastian hukum. Selain itu, aparat penegak hukum kerap menghadapi kesulitan dalam mengkategorikan apakah *doxing* termasuk pencemaran nama baik, pelanggaran data pribadi, atau tindak pidana lain.

Berbeda dengan negara Singapura, melalui *Protection from Harassment Act* (POHA) telah mengatur secara khusus mengenai *doxing*. Amandemen pada tahun 2019 menambahkan ketentuan eksplisit yang melarang *doxing*, dengan beberapa kategori yaitu, pertama mengungkapkan informasi pribadi seseorang dengan maksud untuk melecehkan, mengintimidasi, atau mengancam korban. Kedua, mengungkapkan informasi pribadi seseorang dengan maksud agar orang lain melecehkan atau mengancam korban.

Pelaku *doxing* di bawah POHA dapat dijatuhi sanksi berupa denda hingga SGD 5.000 atau pidana penjara maksimal 6 bulan untuk pelanggaran pertama, dan lebih berat untuk pelanggaran berulang¹³. Selain itu, korban juga dapat mengajukan protection order atau expedited protection order untuk melindungi dirinya dari ancaman lebih lanjut. Singapura dengan demikian telah memberikan

perlindungan hukum yang jelas dan efektif terhadap korban *doxing*, serta memberikan kepastian hukum yang memadai bagi aparat penegak hukum.

Analisis Perbandingan Pengaturan Hukum tentang *Doxing* di Indonesia dan Singapura.

Perbandingan pengaturan hukum terhadap *doxing* antara Indonesia dan Singapura memperlihatkan perbedaan mendasar baik dari sisi normatif, struktural, maupun praktis penegakan hukum.

a. Pendekatan Hukum di Indonesia.

Pertama, di Indonesia tidak terdapat regulasi yang secara eksplisit mengatur tindak pidana *doxing*. Pelaku *doxing* umumnya dijerat dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) atau Undang-Undang Perlindungan Data Pribadi (UU PDP), tergantung pada konteks dan motif pelaku. Namun, kedua undang-undang tersebut tidak secara khusus mengatur *doxing* sebagai tindak pidana tersendiri. Sebagai contoh, dalam kasus hacker Bjorka yang membocorkan data pribadi pejabat publik Indonesia, seperti Menteri Komunikasi dan Informatika Johnny G. Plate dan Menteri Koordinator Bidang Kemaritiman dan Investasi Luhut Binsar Pandjaitan, tindakan tersebut dapat dijerat dengan Pasal 26 UU ITE terkait pengungkapan data pribadi tanpa izin. Namun, tidak ada pasal yang secara spesifik mengatur *doxing* sebagai tindak pidana.

Kedua, kendala dalam penegakan hukum. Penegakan hukum terhadap kasus *doxing* di Indonesia menghadapi beberapa kendala, antara lain: klasifikasi tindak pidana yang tidak jelas, tidak adanya ketentuan spesifik mengenai *doxing* membuat aparat penegak hukum kesulitan dalam mengklasifikasikan dan menindaklanjuti kasus secara konsisten. Kemudian, kesulitan dalam menentukan motif dan tujuan, *doxing* dapat dilakukan

¹² Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang ITE.

<https://anwarpublisher.com/index.php/jic>

¹³ Ministry of Law Singapore, 'Amendments to the Protection from Harassment Act (POHA),' 2019.

dengan berbagai motif, seperti untuk tujuan jahat, kepentingan politik, atau self-regulation. Tanpa klasifikasi yang jelas, penentuan sanksi yang tepat menjadi sulit.

Ketiga, yaitu kurangnya perlindungan hukum bagi korban. Korban *doxing* sering kali tidak mendapatkan perlindungan hukum yang memadai, terutama jika tindakan tersebut belum menimbulkan kerugian fisik langsung. Contoh studi kasus, dalam Kasus Hacker Bjorka. Pada Agustus 2022, hacker yang dikenal dengan nama Bjorka membocorkan data pribadi lebih dari 1,3 miliar pengguna kartu SIM di Indonesia, termasuk data pelanggan Indihome dan dokumen dari Komisi Pemilihan Umum (KPU)¹⁴. Tindakan ini menimbulkan keresahan publik dan mengungkapkan lemahnya sistem keamanan siber di Indonesia¹⁵. Namun, hingga saat ini, belum ada regulasi yang secara spesifik mengatur *doxing* sebagai tindak pidana, sehingga penegakan hukum terhadap pelaku menjadi terbatas¹⁶.

b. Pendekatan Hukum di Singapura

Pertama, Singapura telah mengadopsi pendekatan yang lebih tegas dengan mengatur *doxing* secara eksplisit dalam Protection from Harassment Act (POHA) yang diamendemen pada tahun 2019. Terdapat tiga jenis tindak pidana *doxing* yang diatur, yaitu:

- 1) Mempublikasikan informasi pribadi dengan niat untuk menyebabkan pelecehan, alarm, atau kesusahan: Pelaku dapat dikenakan denda hingga S\$5.000

dan/atau penjara hingga 6 bulan untuk pelanggaran pertama.

- 2) Mempublikasikan informasi pribadi untuk menimbulkan rasa takut akan kekerasan: Pelaku dapat dikenakan denda hingga S\$5.000 dan/atau penjara hingga 12 bulan untuk pelanggaran pertama.
- 3) Mempublikasikan informasi pribadi untuk memfasilitasi penggunaan kekerasan: Pelaku dapat dikenakan denda hingga S\$5.000 dan/atau penjara hingga 12 bulan untuk pelanggaran pertama.

Selain itu, POHA juga memberikan mekanisme perlindungan bagi korban, seperti protection order dan expedited protection order, yang memungkinkan korban untuk segera mendapatkan perlindungan hukum.

Kedua, penegakan hukum yang efektif, dengan adanya regulasi yang jelas dan mekanisme perlindungan yang tersedia, penegakan hukum terhadap kasus *doxing* di Singapura menjadi lebih efektif. Aparat penegak hukum memiliki pedoman yang jelas dalam menangani kasus *doxing*, sehingga proses hukum dapat berjalan dengan lancar dan memberikan efek jera bagi pelaku.

Contoh studi kasus dalam Kasus Penghuni Kondominium di Whampoa. Pada tahun 2019, seorang pria yang difilmkan sedang menyalahkan petugas keamanan kondominium saat hari Deepavali, videonya viral¹⁷. Nomor telepon, unit kondominium, status pekerjaan, dan informasi pribadi lainnya kemudian dipublikasikan secara online oleh warga net¹⁸. Korban melaporkan bahwa informasi pribadi dirinya disebar untuk melecehkan atau mengintimidasi¹⁹. Kasus ini

¹⁴ Ayunda Pininta Kasih, "Data 1,3 Miliar Nomor HP Diduga Bocor Dan Dijual, Kominfo Lakukan Penelusuran," Kompas.com, 2022, <https://tekno.kompas.com/read/2022/09/01/12000087/d-ata-13-miliar-nomor-hp-diduga-bocor-dan-dijual-kominfo-lakukan-penelusuran%0A>.

¹⁵ CNN Indonesia, "Data KPU Diduga Bocor, Bjorka Unggah 105 Juta Data Pemilih," CNN Indonesia, 2022, <https://www.cnnindonesia.com/teknologi/20220906101228-185-842756/data-kpu-diduga-bocor-bjorka-unggah-105-juta-data-pemilih%0A>.

¹⁶ Achmad Dwi Afriyadi, "Bjorka Sebar Data Lagi, Kominfo Kembali Buka Suara," Detik.com, 2022, <https://finance.detik.com/berita-ekonomi-bisnis/d->

<https://anwarpublisher.com/index.php/jic>

6270611/bjorka-sebar-data-lagi-kominfo-kembali-buka-suara%0A.

¹⁷ Shaffiq Alkhatib, "Man Filmed Verbally Abusing Security Officer at Condo Files Police Report 2019," *The Straits Times*, 2019, <https://www.straitstimes.com/singapore/courts-crime/man-filmed-verbally-abusing-security-officer-at-condo-files-police-report%0A>.

¹⁸ Claire Huang, "New Laws to Tackle Doxxing: What You Need to Know," *The Straits Times*, 2020, <https://www.straitstimes.com/singapore/courts-crime/new-laws-to-tackle-doxxing-what-you-need-to-know%0A>.

¹⁹ Ministry of Law Singapore, "Amendments to the Protection from Harassment Act (POHA)," 2019.

merupakan contoh bagaimana POHA di Singapura dapat digunakan untuk menindak pelaku *doxing* dan memberikan perlindungan kepada korban.

Urgensi Pengaturan Khusus *Doxing*

Masalah di Indonesia, *doxing* belum diatur secara eksplisit dalam peraturan perundang-undangan. Pelaku yang melakukan penyebaran data pribadi atau informasi sensitif biasanya dijerat melalui UU ITE atau UU PDP, tergantung konteks tindakannya. Misalnya, penyebaran alamat, NIK, atau informasi pribadi orang lain bisa dikategorikan sebagai pelanggaran Pasal 26 UU ITE terkait data pribadi. Namun, terdapat beberapa kendala dalam penerapan hukum:

a. Klasifikasi Tindak Pidana

Doxing di Indonesia kerap menghadapi kesulitan dalam klasifikasi hukum. Apakah tindakan tersebut termasuk pencemaran nama baik (Pasal 27 ayat 3 UU ITE), pengungkapan data pribadi (Pasal 26 UU ITE), atau pelanggaran UU PDP? Kesulitan ini muncul karena setiap peristiwa *doxing* memiliki konteks yang berbeda, misalnya, tujuan pelaku bisa untuk mengintimidasi, melecehkan, atau sekadar menyebarkan informasi tanpa maksud jahat. Kurangnya ketentuan spesifik membuat aparat penegak hukum harus menafsirkan norma yang ada, sehingga penegakan hukum bisa menjadi tidak konsisten dan lambat.

b. Kepastian Hukum bagi Korban

Korban *doxing* seringkali tidak memiliki perlindungan hukum yang memadai, terutama jika tindakan *doxing* belum menimbulkan kerugian fisik langsung. UU PDP memang memberikan sanksi pidana bagi pelanggaran pengolahan data pribadi, tetapi ketentuan ini bersifat umum dan belum mengakomodasi mekanisme perlindungan cepat seperti *protection order*. Akibatnya, korban sering mengalami kesulitan dalam menghentikan penyebaran data atau mengajukan kompensasi.

c. Aspek Praktis Penegakan Hukum

Penegakan hukum terhadap kasus

doxing di Indonesia juga terkendala oleh anonimitas pelaku. Banyak kasus dilakukan melalui akun anonim di media sosial, sehingga sulit melacak pelaku. Ditambah lagi, kecepatan penyebaran informasi melalui platform digital membuat upaya penegakan hukum tertinggal, sementara kerugian korban sudah terjadi.

Secara normatif, meski hak privasi diakui dalam Pasal 28G UUD 1945, praktik perlindungan hak ini masih terbatas. Hal ini menimbulkan celah hukum yang bisa dimanfaatkan pelaku, sehingga pembentukan regulasi khusus untuk *doxing* menjadi sangat mendesak.

Singapura telah mengambil langkah berbeda dengan menetapkan aturan spesifik mengenai *doxing* melalui *Protection from Harassment Act (POHA)* yang diamendemen pada tahun 2019. POHA mengatur beberapa bentuk *doxing*, termasuk pengungkapan informasi pribadi dengan maksud melecehkan, mengintimidasi, atau mendorong pihak lain untuk melecehkan korban²⁰. Keunggulan pendekatan Singapura antara lain:

a. Kepastian Hukum

POHA memberikan definisi dan ruang lingkup yang jelas mengenai *doxing*. Aparat penegak hukum memiliki dasar hukum yang tegas untuk menindak pelaku, sehingga proses investigasi dan penuntutan lebih terarah. Hal ini berbeda dengan Indonesia, di mana aparat harus menafsirkan norma umum yang belum spesifik.

b. Perlindungan Korban yang Komprehensif

Korban *doxing* di Singapura bisa mengajukan *protection order* atau *expedited protection order* untuk menghentikan penyebaran informasi secara cepat. Mekanisme ini memberikan perlindungan langsung dan efektif bagi korban, termasuk langkah-langkah preventif sebelum kerugian lebih lanjut terjadi.

²⁰ Ibid.

c. Sanksi Hukum Jelas

Pelaku *doxing* di Singapura dapat dikenai sanksi pidana berupa denda atau penjara, tergantung tingkat keseriusan pelanggaran. Dengan adanya sanksi tegas, efek jera lebih jelas dan dapat menekan potensi tindakan serupa di masa depan.

d. Efektivitas Penegakan Hukum

Singapura memiliki aparat hukum yang terbiasa menangani kasus cyber harassment, termasuk *doxing*. Proses pelaporan, investigasi, dan penegakan hukum dilakukan dengan prosedur yang terstandarisasi, sehingga lebih cepat dan efektif dibandingkan di Indonesia.

Beranjak dari uraian di atas, urgensi pengaturan *doxing* di Indonesia dapat dilihat dari beberapa aspek, yaitu aspek normatif privasi diakui sebagai hak asasi yang harus dilindungi oleh negara. Kemudian, aspek praktis yaitu semakin banyak kasus *doxing* terjadi di Indonesia, namun aparat penegak hukum mengalami kesulitan menjerat pelaku, dan aspek komparatif, Singapura telah membuktikan bahwa regulasi khusus memberikan efektivitas perlindungan hukum.

Indonesia saat ini belum memiliki pengaturan khusus yang mengatur *doxing*, sehingga masih bergantung pada UU ITE dan UU PDP yang sifatnya umum. Sebaliknya, Singapura telah lebih progresif dengan mengatur secara eksplisit tindak pidana *doxing* melalui POHA. Perbandingan ini menunjukkan bahwa Indonesia tertinggal dalam memberikan perlindungan hukum yang jelas dan efektif bagi korban *doxing*. Maka dari itu, perlu adanya langkah konkret untuk membentuk regulasi khusus yang mengatur *doxing*, baik dalam bentuk revisi UU ITE maupun melalui undang-undang.

4. Kesimpulan

Secara keseluruhan, perbandingan ini menunjukkan bahwa pendekatan hukum Indonesia masih bersifat umum dan reaktif, sedangkan Singapura lebih spesifik, preventif, dan memberi perlindungan nyata bagi korban. Hal ini menegaskan urgensi revisi UU ITE atau pembentukan regulasi baru yang secara

khusus mengatur *doxing* sebagai tindak pidana siber.

Perbandingan kedua negara menunjukkan beberapa implikasi penting bagi pengembangan hukum di Indonesia:

- a. Perlu Ketentuan Khusus, tanpa pengaturan eksplisit, *doxing* di Indonesia hanya dapat dijerat melalui pasal-pasal umum, sehingga kepastian hukum bagi korban dan aparat penegak hukum terbatas.
- b. Mekanisme Perlindungan Korban, Indonesia perlu mengadopsi mekanisme seperti protection order agar korban dapat menghentikan penyebaran informasi sebelum kerugian lebih lanjut terjadi.
- c. Penegakan Hukum Lebih Cepat dan Tepat Sasaran, POHA memberikan contoh bagaimana aturan yang jelas memungkinkan aparat melakukan investigasi dan penuntutan yang lebih efektif. Indonesia dapat memodifikasi UU ITE dan UU PDP agar memberikan pedoman konkret bagi aparat penegak hukum.
- d. Efek Jera, sanksi tegas di Singapura berfungsi sebagai efek jera. Di Indonesia, ketidakjelasan norma hukum dapat membuat pelaku merasa relatif aman dari risiko hukum, sehingga tindakan *doxing* masih marak.

5. Saran

Perbandingan dengan Singapura menunjukkan bahwa Indonesia perlu segera mengadopsi regulasi yang secara spesifik mengatur tindak pidana *doxing*. Tanpa adanya regulasi yang jelas, penegakan hukum terhadap kasus *doxing* akan terus menghadapi kendala, dan korban akan terus kekurangan perlindungan hukum yang memadai. Dengan demikian, penulis mengajukan beberapa rekomendasi bagi kepastian hukum terkait *doxing* di Indonesia, yaitu:

- a. Pembentukan Regulasi Khusus. Membentuk undang-undang yang secara spesifik mengatur tindak pidana *doxing*, termasuk definisi, unsur-unsur, dan sanksi yang jelas.

- b. Peningkatan Literasi Digital. Meningkatkan literasi digital di kalangan masyarakat untuk mengurangi risiko menjadi korban *doxing*.
- c. Pelatihan bagi Aparat Penegak Hukum. Memberikan pelatihan kepada aparat penegak hukum mengenai penanganan kasus *doxing* agar dapat menindaklanjuti kasus dengan efektif.
- d. Kerjasama Internasional. Meningkatkan kerjasama dengan negara-negara lain dalam menangani kejahatan siber, termasuk *doxing*, mengingat sifatnya yang lintas batas

Dengan adanya regulasi yang jelas dan mekanisme perlindungan yang efektif, diharapkan kasus *doxing* dapat diminimalisir dan korban dapat memperoleh keadilan yang seadil-adilnya

References

- Achmad Dwi Afriyadi. "Bjorka Sebar Data Lagi, Kominfo Kembali Buka Suara." Detik.com, 2022. <https://finance.detik.com/berita-ekonomi-bisnis/d-6270611/bjorka-sebar-data-lagi-kominfo-kembali-buka-suara%0A>.
- Alkhatib, Shaffiq. "Man Filmed Verbally Abusing Security Officer at Condo Files Police Report 2019." The Straits Times, 2019. <https://www.straitstimes.com/singapore/courts-crime/man-filmed-verbally-abusing-security-officer-at-condo-files-police-report%0A>.
- Citron, Danielle Keats. *Hate Crimes in Cyberspace*. Harvard University Press, 2014.
- Douglas, David M. "Doxing: A Conceptual Analysis." *Ethics and Information Technology* 18, no. 3 (2016): 199–210. <https://doi.org/10.1007/s10676-016-9406-0>.
- Faza, M, and R Wiyanti. "Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah." *Jurnal Hukum Siber* 9, no. 1 (2024): 45–60.
- Huang, Claire. "New Laws to Tackle Doxxing: What You Need to Know." The Straits Times, 2020. <https://www.straitstimes.com/singapore/courts-crime/new-laws-to-tackle-doxxing-what-you-need-to-know%0A>.
- Indonesia, CNN. "Data KPU Diduga Bocor, Bjorka Unggah 105 Juta Data Pemilih." CNN Indonesia, 2022. <https://www.cnnindonesia.com/teknologi/20220906101228-185-842756/data-kpu-diduga-bocor-bjorka-unggah-105-juta-data-pemilih%0A>.
- Kasih, Ayunda Pininta. "Data 1,3 Miliar Nomor HP Diduga Bocor Dan Dijual, Kominfo Lakukan Penelusuran." Kompas.com, 2022. <https://tekno.kompas.com/read/2022/09/01/12000087/data-13-miliar-nomor-hp-diduga-bocor-dan-dijual-kominfo-lakukan-penelusuran%0A>.
- Koh, Fabiah. "Budget Debate: 853 Applications for Protection Orders Made since Introduction of Anti-Harassment Law in November 2014." The Straits Times, 2021. <https://www.straitstimes.com/singapore/politics/budget-debate-853-applications-for-protection-orders-made-since-introduction-of>
- Ministry of Law Singapore, "Amendments to the Protection from Harassment Act (POHA)," 2019.
- Ministry of Law Singapore, "Commencement of Protection from Harassment Court on 1 June 2021", press release.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G.
- Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE.
- Yunita, Ernani, Maeda Istiza, and Apriliantoni. "Pentingnya Teknologi Informasi Dan Komunikasi Dalam Sehari-Hari." *El-Idare: Journal of Islamic Education Management* 11, no. 1 (2025): 134–40.

<http://jurnal.radenfatah.ac.id/index.php/E-l-idare>.

Zhang, Laney. "Singapore: Amendment to Harassment Law Passed to Criminalize 'Doxing'." 2019. <https://www.loc.gov/item/global-legal-monitor/2019-10-25/singapore-amendment-to-harassment-law-passed-to-criminalize-doxxing/>.