



PENEGAKAN HUKUM TERHADAP KASUS SIBER DI DITRESKRIMSUS (STUDI KASUS PADA POLDA METRO JAYA TAHUN 2022)

Arga Pardede

Program Magister Kajian Ilmu Kepolisian, Universitas Indonesia

argapardede29@gmail.com

Chairul Muriman Setyabudi

Program Magister Kajian Ilmu Kepolisian, Universitas Indonesia

cak_iir1966@yahoo.com

Surya Nita

Program Magister Kajian Ilmu Kepolisian, Universitas Indonesia

surya.nita@ui.ac.id

Abstrak

Penelitian ini bertujuan untuk mengkaji praktik penegakan hukum terkait pelaku kejahatan siber dan Badan Reserse Kriminal Polda Metro Jaya Tahun 2022. Penelitian ini menggunakan metodologi penelitian hukum normatif yang disempurnakan dengan menggunakan data atau komponen empiris. Temuan penelitian menunjukkan bahwa Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik telah melakukan perubahan terhadap Undang-Undang Nomor 11 Tahun 2008 tentang hal yang sama. Amandemen ini telah memberikan kerangka normatif yang relatif akomodatif untuk memenuhi kebutuhan individu yang melakukan aktivitas di dunia siber. Jenis kejahatan siber yang banyak terjadi di wilayah Polda Metro Jaya antara lain penipuan email, website, dan SMS, akses atau pembajakan data tanpa izin, peretasan, dan pemerasan atau ancaman menggunakan media elektronik. Polisi terlebih dahulu menerima laporan atau pengaduan terkait kejahatan siber, kemudian melakukan penyelidikan untuk memastikan status tersangka terkait penegakan hukum kejahatan siber.

Kata Kunci: Hukum, Ditreskrimsus, Siber, Polisi.

Abstract

The objective of this study is to examine the law enforcement practices pertaining to cyber criminals and the criminal investigation department at Polda Metro Jaya in 2022. This study employs normative legal research methodology, which is enhanced by the use of data or empirical components. The research findings indicate that Law No.19 of 2016, which pertains to Information and Electronic Transactions, has made amendments to Law No. 11 of 2008 on the same subject. These amendments have provided a normative framework that is relatively accommodating to meet the needs of individuals engaging in activities in the cyber world. The prevalent kinds of cybercrime in the Polda Metro Jaya region include email, website, and SMS fraud, unauthorized data access or hijacking, hacking, and extortion or threats using electronic media. The police first receive reports or complaints regarding cyber crimes, and then conduct an investigation to ascertain the suspect's status in relation to law enforcement for cyber crimes. This investigation takes place once clear and direct evidence is available, which can be directly linked to the reported party or their actions.

Keywords: Law, Ditreskrimsus, Cyber, Police.



© Author(s) 2024

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

PENDAHULUAN

Orang-orang percaya bahwa media sosial adalah pengubah permainan dalam hal teknologi informasi dan komunikasi.¹ Dapat dikatakan bahwa internet adalah teknologi terpenting yang pernah diciptakan manusia untuk berkomunikasi dan berbagi informasi. Kemampuan informasi, komunikasi, dan teknologi telah mengalami kemajuan pesat pada saat artikel ini ditulis. Ketergantungan kita pada teknologi semakin meningkat seiring dengan kompleksitas peralatan teknologi komunikasi dan informasi yang kita miliki.²

Seseorang dengan niat buruk memanfaatkan teknologi informasi karena berbagai alasan karena pesatnya kemajuan teknologi dan kebutuhan setiap orang untuk lebih mudah menerima teknologi pada saat tertentu.³ Karena internet adalah media komunikasi virtual yang tidak terlihat, penjahat dapat dengan mudah menghapus jejak tanpa meninggalkan bukti yang jelas, sehingga semakin sulit untuk mengidentifikasi dan menangkap mereka yang bertanggung jawab atas kejahatan paling kompleks dan sulit diselesaikan yang dilakukan melalui internet. media ini.

Tindakan melawan hukum di dunia maya merupakan fenomena yang sangat memprihatinkan karena carding, hacking, penipuan, terorisme, dan transmisi informasi yang merusak semuanya menjadi komponen kejahatan dunia maya. Berbeda sekali dengan fakta ini, saat ini tidak ada peraturan yang mengatur bagaimana berbagai industri harus menggunakan ICT. Oleh karena itu, pemerintah harus menetapkan aturan tersebut guna menjamin keselamatan masyarakat.⁴

Penegakan hukum pidana, khususnya yang berkaitan dengan kejahatan yang dilakukan melalui penggunaan teknologi digital, sangat terbantu dengan adanya peraturan perundang-undangan yang berkaitan dengan regulasi Cyber Crime. Fakta bahwa kejahatan dunia maya merupakan hal yang umum di Indonesia membuktikan pentingnya peraturan ini. Orang-orang yang memanfaatkan sumber daya online untuk mengkritik pemerintah akan mendapat masalah hukum ketika UU ITE diberlakukan dan hukuman pidana diterapkan. Hal tersebut di atas merupakan hasil dari pengaturan UU ITE mengenai kejahatan dunia maya sebagaimana didefinisikan dalam Konvensi Kejahatan Dunia Maya dan kejahatan pidana yang dilakukan melalui penghinaan online.

Terdapat peningkatan substansial dalam kejahatan dunia maya pada tahun 2022 dibandingkan dengan tahun yang sama pada tahun 2021. Jumlah kejahatan dunia maya meningkat empat kali lipat. Sejak 1 Januari 2022 hingga 22 Desember 2022, terdapat 8.831 peristiwa kejahatan

¹ Ruth Gladys Sembiring dkk., "Penegakan Hukum Cybercrime di Wilayah Hukum Kepolisian Daerah Sumatera Utara," *Locus Journal of Academic Literature Review*, 2023, 292–304.

² Herio Ramadhona, "Penggunaan Platform Aplikasi Only Fans untuk Cyber-Pornografi (Studi Kasus Deaonly Fans di Polda Metro Jaya)," *Jurnal Impresi Indonesia* 1, no. 10 (2022): 1102–8.

³ Alyfia Syavira, "Analisis Perlindungan Hukum Terhadap Korban Kejahatan Doxing (Studi pada Polda Metro Jaya)," 2022.

⁴ Prasetyo Prasetyo dan Mukhtar Zuhdy, "Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, no. 2 (2020): 79–88.

siber yang telah diinvestigasi dan dituntut berdasarkan data e-MP Robinopsnal Bareskrim Polri. Secara keseluruhan, Bareskrim Polri dan Kepolisian Daerah Republik Indonesia merespons kejadian tersebut. Dari 3.709 kasus kejahatan siber yang ditindak, Polda Metro Jaya memiliki jumlah kasus terbanyak. Polri mengakui bahwa tidak mudah untuk merespons kasus-kasus kejahatan dunia maya. Contoh ini ditangani secara berbeda dari yang lain. Untuk itu, Polri terus berupaya membentuk Direktorat Cyber Crime di lingkungan kepolisian daerah masing-masing.⁵

Peretasan situs DPR terjadi sebagai kejahatan dunia maya; para pelaku mengubah nama mereka menjadi Dewan Pengkhianat Rakyat. Peretasan yang terjadi pada Kamis, 10 Agustus di situs DPR RI sebenarnya bukan kejadian pertama di tahun 2020. Situs DPR RI tidak bisa dijangkau pada Juni 2020 akibat peretasan. Pada hari Kamis, peretas mendapatkan akses tidak sah ke situs DPR RI dan mengubah desain halaman utamanya. Situs yang disusupi ini milik organisasi pemerintah terkemuka dan dapat diakses di dpr.go.id. Setelah berganti nama dari Dewan Perwakilan Rakyat Republik Indonesia menjadi Dewan Pengkhianat Rakyat, maka diambillah akronim DPR. Hal ini menarik perhatian netizen Indonesia ketika website DPR RI diretas hingga menjadi Dewan Pengkhianat Rakyat.⁶ Kasus Indra Kenz adalah contoh lain kejahatan dunia maya yang menggunakan influencer dan aplikasi Binomo untuk investasi palsu. Indra Kusuma atau Indra Kenz ditetapkan sebagai tersangka pada 24 Februari 2022 oleh Bareskrim Polri. Influencer Indra Kenz mendukung aplikasi Binomo sebagai afiliasi atau pihak ketiga. Indra Kenz menghadapi tuduhan pencucian uang dan pelanggaran Undang-Undang Informasi dan Transaksi Elektronik (ITE), yang berpotensi terancam hukuman penjara 20 tahun. Dengan menggunakan pengetahuan tim Cyber Crime dan dukungan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), pihak berwenang mengklaim dapat melacak penipuan dan jaringan TPPU ini.⁷

Kejahatan dunia maya semakin mendapat perhatian dari penegak hukum dan pembuat undang-undang, seperti yang dibahas di bagian sebelumnya. Potensi kerugian yang diakibatkan oleh penggunaan IT yang ceroboh memerlukan peraturan yang membatasi dan menghukum perilaku tersebut. penggunaan komputer dan internet untuk tujuan ilegal, karena Cyber Crime dalam segala manifestasinya memerlukan retribusi. Polisi sebagai individu yang diberi wewenang oleh undang-undang untuk menegakkan sistem peradilan pidana harus siap menangani berbagai bentuk kejahatan siber. Terkait kejahatan yang menggunakan teknologi informasi, polisi mempunyai kewenangan untuk menyelidiki dan mengusut. Sesuai Pasal 42 Undang-Undang Nomor 11 Tahun

⁵ Pusiknas Bareskrim Polri, "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat," *Pusiknas. Polri. Go. Id.* https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat, 2022.

⁶ U Abdullah Mumin, "The Role of Information Technology in Education World (Peran Teknologi Informasi Dalam Bidang Pendidikan; E-education)," *Al-Afkar, Journal for Islamic Studies*, 2019, 104–19.

⁷ Tsarina Maharani, "Kasus Penipuan Binomo: Indra Kenz Jadi Tersangka, Doni Salmanan Dilaporkan," *Retrieved Maret 21 (2022): 2022*.

2008 tentang Informasi dan Transaksi Elektronik, penyidikan tindak pidana yang memanfaatkan IT dilakukan sesuai dengan aturan hukum acara pidana.

Direktorat II Perekonomian dan Unit Khusus V IT dan Cyber Crime, unit khusus di Badan Reserse Kriminal (BARESKRIM) Mabes Polri, serta Unit Pencegahan Cyber Crime di sejumlah instansi Kepolisian Daerah (Polda), bertanggung jawab untuk memberantas kejahatan yang melibatkan teknologi informasi. Unit khusus di bidang teknologi informasi telah dikembangkan oleh kepolisian daerah seperti Polda Metro Jaya. Landasan unit ini didorong oleh keinginan untuk mengatasi dan mencegah kejahatan dengan menggunakan teknologi informasi. Provinsi ini berharap kelompok-kelompok yang baru terbentuk ini mampu memberantas kejahatan yang dilakukan dengan menggunakan teknologi informasi. Meskipun Subdit IV/Cyber Crime menangani kejahatan siber, Direktorat Reserse Kriminal Khusus Polda Metro Jaya berperan penting dalam penegakan hukum secara umum. Pada tahun 2022, Ditreskrimsus Polda Metro Jaya memanfaatkan data pelanggaran siber.

Tujuan dari kajian dan penelitian penegakan hukum di Polda Metro Jaya terkait dengan kejahatan siber dan tindak pidana adalah untuk menjelaskan proses yang dilakukan penyidik kejahatan siber dalam memastikan waktu dan lokasi kejadian, serta untuk memfasilitasi pekerjaan mereka dan memajukan bidang hukum pidana mengenai kejahatan dunia maya dan tantangan yang dihadapi oleh penyidik dalam mencari solusi.

METODE PENELITIAN

Riset ini menggunakan penelitian hukum normatif dan data tambahan atau komponen empiris. Sifat analitis dan konseptual kajian hukum normatif membedakannya dengan cabang hukum lainnya. Konsep, doktrin, undang-undang, dan standar hukum merupakan fokus utama dari pendekatan ini. Kajian hukum normatif berupaya memahami tidak hanya bentuk dan isi norma hukum tetapi juga landasan teoretis dan kegunaan praktisnya.⁸ Penelitian ini bercirikan pendekatan deskriptif dan analitis. Data diambil dari sumber primer dan sekunder. Data primer dikumpulkan melalui wawancara mendalam dengan sumber literatur primer Polda Metro Jaya yang relevan langsung dengan objek penelitian. Sedangkan data sekunder berasal dari berbagai sumber perpustakaan, termasuk bahan hukum primer, sekunder, dan tersier. Metode dari tinjauan literatur dan penelitian lapangan berkontribusi pada pengumpulan data ini. Prosesnya dimulai dengan pengumpulan data dan dilanjutkan dengan analisis kualitatif, yang mengarah pada kesimpulan deduktif. Temuan-temuan ini kemudian dideskripsikan atau diinterpretasikan dengan menggunakan bahasa yang informatif dan persuasif.

⁸ Nanda Dwi Rizkia dan Hardi Fardiansyah, “Metode Penelitian Hukum (Normatif dan Empiris),” 2023.

HASIL DAN PEMBAHASAN

UU Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016 Mengatur Kejahatan Dunia Maya dengan Perubahan UU Nomor 11 Tahun 2008

Dengan disahkannya Rancangan Undang-Undang Informasi dan Transaksi Elektronik dan selanjutnya diundangkan menjadi Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Indonesia telah memasuki babak baru dalam pengaturan penggunaan teknologi informasi dan transaksi elektronik sejak saat itu. 21 April 2008. (UU RI No. 58 Tahun 2008; Peraturan RI No. 4843). Pada tahun 2008, undang-undang pertama di Indonesia yang menangani kejahatan dunia maya adalah undang-undang Nomor 11, yang juga dikenal sebagai UU-ITE, yang merupakan singkatan dari Informasi dan Transaksi Elektronik. Penyusunan dan pemberlakuan undang-undang ini merupakan peristiwa tersendiri. Dengan judul kerja RUU Komunikasi Informasi dan Transaksi Elektronik, Kementerian Negara Komunikasi dan Informatika mulai membahas UU-ITE pada Maret 2003.⁹

Dua kementerian Indonesia (Departemen Perhubungan dan Departemen Perindustrian dan Perdagangan) bersama dengan Lembaga Kajian Hukum dan Teknologi Universitas Indonesia, kelompok dari Fakultas Hukum Universitas Padjadjaran, dan Institut Teknologi Bandung bekerja sama untuk merancang rancangan undang-undang tersebut. versi asli dari RUU ini.¹⁰ Kemudian menanggapi surat resmi Presiden Indonesia. Penyerahan naskah UU-ITE secara resmi kepada DPR RI dilakukan pada tanggal 5 September 2005 berdasarkan Nomor R./70/Pres/9/2005. Undang-undang ini disetujui pada tanggal 21 April 2008; Jadi, proses diundangkannya UU-ITE sudah berjalan hampir lima tahun. Undang-undang yang relatif baru ini, baik dari segi diundangkan maupun diatur dalam isi undang-undang, mempunyai tiga belas bab dan lima puluh empat ketentuan. Mengingat Indonesia merupakan salah satu negara yang banyak memanfaatkan teknologi informasi tanpa mengaturnya secara memadai, khususnya dalam bidang hukum pidana, maka Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi sangat penting bagi pemerintahan negara tersebut.¹¹

Hukum siber pertama di Indonesia yang mengendalikan informasi dan transaksi elektronik adalah Undang-Undang Informasi dan Transaksi Elektronik yang sering dikenal dengan UU ITE. Isi UU ITE ada dua bagian utama: pertama, aturan yang mengatur informasi dan transaksi elektronik; dan kedua, aturan yang mengatur kegiatan ilegal (Cyber Crime). Banyak negara menggunakan peraturan kejahatan dunia maya sebagai alat dalam skala global. Dua bidang utama

⁹ Mumin, "The Role of Information Technology in Education World (Peran Teknologi Informasi Dalam Bidang Pendidikan; E-education)."

¹⁰ S H Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Prenada Media, 2022).

¹¹ Bambang Sutrisno dan F X Bhirawa Braja Paksa, "Penegakan Hukum Terhadap Tindak Pidana Pencemaran Nama Baik Menurut Pasal 27 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Uu Ite)," *Mizan: Jurnal Ilmu Hukum* 8, no. 1 (2019): 20–26.

yang diatur dalam UU ITE adalah kejahatan dunia maya dan pengaturan transaksi elektronik. Dokumen dan informasi elektronik, tanda tangan dan sertifikat elektronik, penatausahaan sistem elektronik, transaksi elektronik, privasi dan hak kekayaan intelektual, ketentuan pidana mengenai penggunaan informasi dan transaksi elektronik, dan sebagainya, semuanya merupakan bagian dari materi UU ITE, yang merupakan bagian dari materi UU ITE. penerapan berbagai prinsip ketentuan internasional.

Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disahkan dengan Undang-undang Nomor 19 Tahun 2016 yang mengatur hal yang sama. Belum ada revisi terhadap jenis kejahatan dunia maya yang dikendalikan; Oleh karena itu, segala jenis kejahatan siber masih diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.¹²

Kejahatan dunia maya tidak didefinisikan oleh hukum di Indonesia. Istilah “Cyber Crime” didefinisikan dalam Undang-Undang Nomor 11 Tahun 2008 yang mengubah Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Kejahatan dunia maya, penipuan email, dan bentuk kejahatan elektronik lainnya didefinisikan dalam UU ITE. Tujuh kategori kegiatan kriminal yang berbeda didefinisikan dalam Undang-Undang Informasi dan Transaksi Elektronik sebagai kejahatan yang dilakukan dengan atau dengan cara elektronik. Kejahatan-kejahatan tersebut dipandang sebagai contoh kriminalitas modern yang memunculkan jenis kriminalitas lainnya.

Berbagai jenis kejahatan dunia maya ditangani berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Berikut adalah berbagai bentuk kejahatan dunia maya yang termasuk dalam lingkup UU ITE dan berdampak pada sistem elektronik:

1. Pencurian Identitas (Pasal 30 UU ITE): akses tidak sah atau kepemilikan data elektronik orang lain, termasuk informasi sensitif seperti kredensial login, dianggap sebagai pencurian identitas.
2. Penyebaran Misinformasi (UU ITE Pasal 14 dan 28): Menyebarkan misinformasi atau berita bohong melalui media elektronik dengan tujuan meresahkan masyarakat.
3. Pasal 4 dan 29 UU ITE mengatur tentang penyebaran atau pembuatan materi pornografi dengan menggunakan sarana elektronik yang dapat diakses publik.
4. Pasal 27 dan 45 UU ITE mengatur penggunaan media elektronik untuk menghina atau mencemarkan nama baik orang lain.

¹² Jeremy Samuel Pangkey Sondakh, “Pemberlakuan Ketentuan Pidana Dalam Pasal 27 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,” *Lex Privatum* 9, no. 5 (2021).

5. Ancaman (UU ITE Pasal 29 dan 45): Pelecehan terhadap orang lain melalui sarana elektronik, seperti media sosial, email, atau pesan teks.
6. Akses Tidak Sah (UU ITE Pasal 30): Merugikan pemilik suatu sistem komputer atau jaringan dengan melakukan peretasan tanpa izin.
7. Pasal 35 UU ITE mendefinisikan G. Fraud sebagai penggunaan identitas palsu atau manipulasi data elektronik secara curang.
8. *Hacking* (UU ITE Pasal 30 dan 46): Memasuki atau mencoba memasuki suatu sistem atau jaringan komputer dengan maksud untuk merugikan atau menguasainya.
9. Kejahatan Dunia Maya dan Penyebarannya (UU ITE Pasal 30): Kejahatan dunia maya dan penyebarannya mencakup penyebaran malware seperti virus, worm, trojan, dan lainnya yang dapat merusak atau melemahkan sistem atau jaringan komputer.
10. Pencurian Data (Pasal 30 UU ITE): Akses tidak sah dan pencurian data atau informasi elektronik orang lain.

Dari sisi hukum, khususnya dalam ranah hukum pidana, UU ITE (UU Informasi dan Transaksi Elektronik) di Indonesia telah membawa beberapa inovasi yang signifikan. Dari sudut pandang hukum, terdapat sejumlah keistimewaan dan kemajuan yang patut diperhatikan, antara lain:

1. Hukum Kejahatan Dunia Maya. Alat legislatif utama untuk mengendalikan berbagai jenis kejahatan dunia maya adalah UU ITE. Ini mencakup berbagai pelanggaran online, termasuk penipuan, peretasan, pencurian identitas, dan lain-lain.
2. Kesesuaian dengan Standar Internasional. Dalam menangani kejahatan dunia maya, UU ITE mengakui pentingnya kolaborasi internasional. Untuk menyelaraskan denda dengan negara-negara yang memiliki perjanjian atau ketetapan internasional yang berlaku, UU ITE memberikan kewenangan untuk melakukan hal tersebut berdasarkan Pasal 49.
3. Imunitas Subjek Data (UU ITE Pasal 26). Informasi pribadi individu dilindungi berdasarkan UU ITE. Sesuai aturan yang dituangkan dalam UU ITE, terdapat sanksi pidana atas penyalahgunaan atau akses tidak sah terhadap data pribadi.
4. Mengelola Konten Secara Elektronik. Penyebaran materi yang melanggar norma agama, kesusilaan, hukum, atau kesusilaan dilarang berdasarkan Pasal 27 UU ITE. Terdapat konsekuensi pidana atas pelanggaran.
5. Melindungi Anak. Aspek perlindungan terhadap anak di bawah umur masuk dalam UU ITE. Sesuai Pasal 4 dan Pasal 29 UU ITE, terdapat sanksi pidana bagi penyebaran materi pornografi anak melalui sarana elektronik.

6. Pasal 33 UU ITE tentang penyidikan elektronik. Untuk menemukan kejahatan dunia maya, UU ITE memberikan kewenangan kepada penegak hukum untuk melakukan investigasi elektronik.
7. Sistem Hukuman Pidana yang Sangat Ketat. Sanksi pidana yang tegas dituangkan dalam UU ITE bagi siapa pun yang melakukan kejahatan dunia maya. Hukuman dapat berkisar dari denda hingga hukuman penjara, tergantung pada keseriusan pelanggaran dan tingkat kesalahan pelaku.
8. Pasal 30 UU ITE mengatur upaya pencegahan. UU ITE mengatur sanksi pidana dan tindakan pencegahan, seperti pemblokiran akses ke situs web atau materi yang melanggar hukum.
9. Pasal 76 UU ITE mengatur tentang tindakan ganti rugi. UU ITE mengatur tata cara pemberian kompensasi kepada individu atau badan yang dirugikan akibat pelanggaran UU ITE. Kerugian yang berwujud maupun tidak berwujud termasuk di dalamnya.
10. Pasal 29 UU ITE mengatur ketentuan yang bertujuan untuk memberantas terorisme. Cara lain UU ITE membantu mengakhiri serangan teroris adalah dengan melarang penyebaran informasi apa pun tentang kejahatan tersebut.

Secara umum, dalam hal pengaturan kejahatan siber, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) cukup akomodatif dalam memenuhi kebutuhan masyarakat dalam melakukan aktivitas siber. Ketentuan baik substansi maupun prosesnya telah dituangkan dalam UU ITE. Oleh karena itu, UU ITE memastikan dan memberikan kejelasan hukum dalam pelaksanaan operasional melalui EIS. Dunia maya merupakan dunia maya yang sulit ditemukan di dunia nyata namun dapat diakses kapan saja oleh jutaan pengguna di seluruh dunia,¹³ sehingga sulit untuk menjinakkan kejahatan ini bahkan setelah berlakunya UU ITE. di Indonesia di dunia cyber. Karena kualitas ini, UU ITE mengalami kesulitan dalam pemberlakuannya, dan permasalahan yurisdiksi hukum yang cacat masih terus terjadi hingga saat ini. Dilema mengenai negara mana yang mempunyai otoritas atas kejahatan dunia maya dan dampaknya muncul karena kejahatan dunia maya seringkali melintasi batas-batas internasional. Untuk mengatasi masalah ini dalam batas-batas hukum, Indonesia telah memutuskan untuk merevisi kerangka hukumnya untuk melindungi kedaulatan nasional, kebebasan individu, dan kepentingan seluruh rakyat Indonesia.

¹³ Sembiring dkk., "Penegakan Hukum Cybercrime di Wilayah Hukum Kepolisian Daerah Sumatera Utara."

Penegakan Hukum Kejahatan Siber di Wilayah Kepolisian Daerah Metropolitan Jakarta Raya

Berdasarkan hasil penelitian lapangan maka diperoleh data tentang bentuk-bentuk tindak pidana siber di lingkungan Polda Metro Jaya dari bulan Januari hingga Desember 2022 sebagaimana berikut:

Tabel 1.
Rekapitulasi Data Tindak Pidana Cyber di Polda Metro Jaya

No	Jenis Tindak Pidana	Bulan											
		J n	F b	M r	Ap	M e	Jn	Jl	A g	S p	O k	N v	D s
1	Kejahatan terhadap Kesusilaan dan Kesopanan/Pornografi online	2	3	2	1	1	3	3	5	1	6	3	1
2	Pencemaran nama baik / penghinaan melalui internet/Perbuatan tidak menyenangkan	3	4	6	8	2	11	1	4	1	2	5	3
3	Penjebolan / pengrusakan dan penggunaan email atau password/ Pengrusakan data	0	0	0	0	16	20	0	1	0	0	0	0
4	Penipuan melalui email, website, dan sms	40	35	46	50	26	41	28	22	16	23	34	18
5	Perjudian online	0	0	0	0	0	0	0	4	1	0	0	1
6	Penggelapan	0	0	0	0	0	0	0	0	0	0	0	1
7	Pencurian data/ carding/Pemindahan data (pasal 32 uu ite)	1	0	0	0	0	1	1	4	1	1	0	0
8	Pencurian ATM	0	0	0	0	0	0	0	0	0	0	0	0
9	Pemerasan/Pengancamann melalui media elektronik	10	5	7	7	9	13	11	7	5	3	4	11
10	Memanipulasi data	3	8	3	3	8	4	1	4	2	2	4	0
11	Mengakses / Membajak data orang lain/Hack	35	17	9	29	1	0	19	13	19	14	23	4
12	Memindahkan / Mentransfer informasi tnp ijin	1	2	1	1	0	0	0	0	0	0	0	0
13	Menghilangkan data	0	0	0	0	0	0	0	0	0	0	0	0
14	Pemalsuan data/email (pasal 263 kuhp/pasal 28 ayat 1 uu ite)	0	0	0	0	0	0	0	0	0	0	0	0
15	Penyiaran	0	0	0	0	0	0	0	0	0	0	0	0
16	Menyebarkan berita bohong/ HOAX	1	0	1	0	1	4	1	0	2	0	3	0

17	Menyebarkan <i>informasi yang menimbulkan kebencian</i> dan SARA (pasal 28 ayat 2 uu ite)	2	0	0	1	1	4	4	8	0	1	2	0
18	Penghinaan melalui media elektronik	0	0	0	0	0	0	0	0	0	0	0	0
19	Penghinaan lambang Negara	0	0	0	0	0	0	0	0	0	0	0	0
20	Penyalahgunaan data	0	0	0	0	0	0	0	0	0	0	0	0
21	Kejahatan terhadap anak	0	0	0	0	0	0	0	0	0	0	0	0
22	TP. Hak Cipta / konsumen	0	2	0	0	0	0	0	0	0	0	0	1
23	Penipuan dan Penggelapan	0	5	0	0	4	0	9	4	5	8	4	2
24	Lain-Lain	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL		98	81	75	100	69	101	78	76	53	60	82	42

Sumber: Ditreskrimsus Polda Metro Jaya, 2022

Tabel 1 menunjukkan bahwa data kasus Cyber dari bulan Januari sampai Desember 2022, tindak pidana Cyber yang paling banyak terjadi ialah pada bulan Juni. Secara keseluruhan, pada bulan Januari hingga Desember 2022 tindak pidana Cyber yang paling sering terjadi ialah penipuan melalui email, website, dan sms, selanjutnya diurutkan kedua terbanyak ialah mengakses/ membajak data orang lain/ hack dan diikuti oleh tindak pidana pemerasan/ pengancaman melalui media elektronik. Pada bulan April hingga Juni tahun 2022 terhitung adanya peningkatan pada jumlah tindak pidana Cyber dan pada bulan Juli hingga Desember tahun 2022, tindak pidana Cyber cenderung mengalami penurunan. Polda Metro Jaya menunjukkan penurunan kasus berbagai kejahatan siber yang menjadi bukti penegakan hukum yang efektif.

Penyidik sering kali mendapatkan banyak petunjuk saat menyelidiki kasus kejahatan dunia maya. Dalam mengidentifikasi pelaku, seringkali pelaku menggunakan nama samaran dibandingkan namanya sendiri. Karena penjahat dunia maya dapat berkeliaran dengan bebas saat melakukan kejahatan, menentukan dengan tepat di mana kejahatan tersebut terjadi dapat menjadi sebuah tantangan. Kasus pencemaran nama baik atau ujaran kebencian di media sosial, misalnya, mengharuskan penyidik berkonsultasi dengan ahli bahasa untuk menentukan validitas pernyataan apa pun yang dibuat di platform tersebut (seperti yang dikatakan dalam wawancara dengan Victor). Saat menyelidiki kemungkinan terjadinya ujaran kebencian, penyidik mungkin perlu berkonsultasi dengan pengacara yang berspesialisasi dalam hukum pidana untuk memastikan tanpa keraguan bahwa pernyataan atau tindakan tersebut merupakan tindakan ilegal.

Seperti yang dikatakan Victor dalam wawancara tersebut, berikut adalah beberapa masalah yang dihadapi pihak berwenang ketika mencoba memerangi penipuan internet:

1. Untuk menutupi jejak mereka dan tetap anonim, penjahat sering kali menggunakan metode teknologi canggih. Polisi kesulitan mengidentifikasi dan melacak pihak-pihak yang bertanggung jawab atas penipuan internet karena maraknya jaringan anonim dan teknologi enkripsi.
2. Cara tradisional untuk memantau penggunaan uang digital dan sistem pembayaran online tidak memberikan kemudahan. Akibatnya, akan lebih sulit bagi penegak hukum untuk melacak pergerakan dana dan menangkap mereka yang bertanggung jawab.
3. Penipu *online* selalu punya strategi baru. Karena adanya evolusi yang terus-menerus dalam tindakan penipuan dan keamanan, lembaga penegak hukum harus meningkatkan keterampilan mereka secara berkala agar dapat mengimbangnya.
4. Menanggapi ancaman dunia maya merupakan tantangan bagi polisi karena kurangnya personel dan pengetahuan teknologi. Investigasi dan penanganan insiden penipuan internet memerlukan kemampuan khusus. Bukti digital yang dapat diterima di pengadilan harus dikumpulkan untuk menyelidiki insiden penipuan internet. Terkait analisis forensik digital, tidak semua lembaga kepolisian memiliki kemampuan yang diperlukan. Saat menyelidiki kasus penipuan, polisi memerlukan akses terhadap data pribadi, namun mereka harus mematuhi undang-undang terkait privasi. Hal ini cenderung menjadi masalah.
5. Saat merespons kejahatan dunia maya, aparat penegak hukum mengalami kesulitan karena kurangnya pengetahuan teknologi.
6. Masyarakat umum masih belum cukup mengetahui tentang bahaya penipuan internet dan cara melaporkannya. Karena malu atau tidak percaya pada polisi, beberapa korban mungkin ragu untuk mengungkapkan kejahatannya.

Temuan dari penelitian menunjukkan bahwa ada beberapa hambatan dalam memberantas kejahatan dunia maya. Setelah mengumpulkan data dari wawancara dan sumber lainnya, penulis mengelompokkannya ke dalam beberapa kategori, antara lain:

1. Faktor Sumber Daya Manusia

Diperlukan jumlah personel investigasi dan penyelidik yang cukup dengan keterampilan yang tepat di setiap unit kejahatan siber jika masyarakat ingin percaya pada upaya polisi untuk memerangi kejahatan siber. Kehadiran unit tersebut dalam penegakan hukum menunjukkan perlunya penyelidik khusus yang memiliki pengetahuan teknologi informasi dan transaksi elektronik untuk menangani kejahatan dunia maya secara efektif.

2. Faktor Pertimbangan Bukti Kejahatan Dunia Maya

Alat bukti dalam kejahatan siber berbeda dengan alat bukti dalam kejahatan tradisional, dimana sasaran atau media kejahatan siber adalah data atau sistem elektronik yang terkoneksi internet. Mengingat hampir setiap orang memiliki telepon genggam

(*Handphone*) dan fasilitas umum lainnya, penyidik menghadapi tantangan unik. Studi kasus ini akan menggunakan data dan hasil wawancara untuk menjelaskan secara rinci hambatan pembuktian dalam kasus kejahatan dunia maya. Banyak sekali permasalahan yang berkaitan dengan kejahatan dunia maya, termasuk fakta bahwa pelaku kejahatan sering kali memanfaatkan sumber daya publik untuk melakukan kejahatannya dan fakta bahwa bukti digital mudah dihapus jika tidak ditangani dengan benar. misalnya, bukti digital mungkin akan hilang jika tidak segera ditangani. Selain itu, pelaku kejahatan siber melakukan aksinya dengan menggunakan ruang publik, dan terdapat saksi yang tidak hadir pada saat kejadian.¹⁴

3. Faktor Fasilitas

Terkait kejahatan dunia maya, laboratorium forensik komputer adalah alat penting bagi penegak hukum dan penyidik. Lab ini dapat menguraikan data digital dan menyimpan bukti dalam bentuk *file softcopy*, termasuk gambar, program, HTML, audio, dan lainnya. Forensik komputer, terkadang disebut forensik digital, adalah studi dan analisis bukti digital dengan tujuan utama mengumpulkan dan melestarikan fakta obyektif mengenai insiden atau pelanggaran keamanan yang melibatkan sistem komputer untuk digunakan dalam proses peradilan. Penyidik dapat mempelajari identitas pengirim (termasuk alamat IP), waktu dan lokasi pembuatan email (menurut server pengirim), dan bahkan lokasi fisik pengunjung dan jenis perangkat yang mereka gunakan (semua berkat forensik internet) dieksekusi menggunakan *platform online*.

4. Faktor Masyarakat

Dari sudut pandang masyarakat, terdapat tantangan seperti kurangnya kepedulian pelanggan saat membeli secara online dan maraknya penipuan media sosial akibat meningkatnya permintaan, yang semuanya mudah dipalsukan. Semakin maju teknologi dan semakin terampil pelaku dalam menggunakan media sosial, maka semakin sulit bagi Polda Metro Jaya untuk menyelesaikan kasus tersebut dan menjamin pelaku akan mengurungkan niatnya untuk mengulangi perbuatannya. Masyarakat harus lebih berhati-hati saat melakukan pembelian secara online; di sinilah peran masyarakat. Ketika masyarakat mengalami kerugian yang besar, mereka sering kali melapor ke polisi untuk meminta bantuan. Masyarakat sering kali menahan diri untuk tidak melaporkan kejadian kepada polisi jika kerugian yang dialami masyarakat relatif kecil. Hal ini disebabkan adanya keyakinan bahwa prosedurnya akan lebih rumit.

¹⁴ Khalissa Aliya Indriany, "Upaya Penanggulangan Tindak Pidana Pelecehan Seksual Anak di Media Sosial (Studi di Kepolisian Daerah Polda Metro Jaya)," *Inovasi Pembangunan: Jurnal Kelitbangan* 11, no. 01 (2023): 87; Aqmarina Khusnul Baiti, "Teknik Pengungkapan Kasus Pinjaman Online (Pinjol) Ilegal di Wilayah DKI Jakarta (Studi Kasus di Polda Metro Jaya)" (Universitas Jenderal Soedirman, 2022).

Menurut penyidik Polda Metro Jaya, upaya untuk mengatasi kendala dalam memberantas kejahatan siber juga dilakukan sebagai berikut: (1) meningkatkan pengetahuan dan kemampuan tim ahli siber agar dapat lebih memahami dan menangkal ancaman siber yang terus terjadi. (1) Memberikan edukasi kepada masyarakat tentang bahaya kejahatan dunia maya, cara tetap aman dalam menggunakan internet, dan apa yang harus dilakukan jika menjadi korban kejahatan dunia maya; (2) Melatih petugas polisi secara teratur untuk selalu mengetahui informasi terkini tentang taktik kejahatan dunia maya dan metode investigasi digital; (3) Memasukkan keamanan siber dalam investigasi kejahatan tradisional untuk mengatasi ancaman siber; (4) Menjangkau masyarakat dan mendidik mereka tentang kejahatan dunia maya; (5) Menciptakan undang-undang dan kebijakan yang mengatasi kejahatan dunia maya dan memberikan landasan hukum yang kokoh bagi penegakan hukum; dan (6) Bekerja sama dengan penyedia layanan *online*, *bank*, dan sektor swasta lainnya untuk berbagi informasi tentang ancaman dunia maya dan berupaya mencegah, merintangi, dan menghalangi pelaku kejahatan untuk melakukan kegiatan ilegal, khususnya kejahatan dunia maya, dengan penggunaan sumber daya yang optimal.

KESIMPULAN

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang mengubah Undang-Undang No. 11 Tahun 2008 tentang hal tersebut, secara normatif dapat disesuaikan dalam memenuhi tuntutan masyarakat dalam menjalankan usaha di dunia Cyber. Selain itu, pada bulan Januari hingga Desember 2022, jenis kejahatan siber yang paling banyak terjadi di wilayah Polda Metro Jaya antara lain: penipuan melalui email, website, dan sms, mengakses/membajak data orang lain/hack, serta pemerasan/pengancaman melalui media elektronik. Penelitian menunjukkan bahwa polisi berperan penting dalam penegakan hukum kejahatan siber, khususnya di wilayah Polda Metro Jaya. Setelah menerima laporan atau pengaduan kejahatan siber, polisi melakukan penyelidikan untuk memastikan apakah yang dilaporkan merupakan tersangka kejahatan siber tersebut setelah bukti nyata mengenai orang atau badan yang dituduhkan telah ditemukan. Bukti fisik, keterangan saksi dan korban, keterangan saksi ahli, dan keterangan terlapor, semuanya merupakan bagian dari proses pembuktian bahwa orang yang bersangkutan adalah tersangka (pelaku). Aspek sumber daya manusia, bukti kejahatan siber, fasilitas, dan masyarakat adalah kendala yang menghambat upaya pemberantasan kejahatan siber di wilayah Polda Metro Jaya. Untuk memerangi kejahatan siber, Polda Metro Jaya berupaya meningkatkan pengetahuan dan kemampuan tim ahli siber, mendidik petugas polisi secara teratur tentang siber dan teknologi, mengintegrasikan langkah-langkah keamanan siber, mengedukasi masyarakat dan melakukan program sosialisasi, membuat undang-undang yang mengatasi dinamika kejahatan siber, dan memberikan penegakan hukum landasan hukum yang kuat, dan berkolaborasi

dengan perusahaan swasta, lembaga keuangan, dan penyedia layanan online untuk berbagi informasi tentang ancaman dunia maya dan melakukan penyelidikan.

Polda Metro Jaya perlu mengadopsi pendekatan yang adaptif dan proaktif dalam menanggapi ancaman kejahatan siber yang terus berkembang. Kolaborasi dan koordinasi yang kuat antara sektor publik dan swasta, serta pemberdayaan masyarakat, akan menjadi kunci keberhasilan dalam memberantas kejahatan siber.

DAFTAR PUSTAKA

- Baiti, Aqmarina Khusnul. "Teknik Pengungkapan Kasus Pinjaman Online (Pinjol) Ilegal di Wilayah DKI Jakarta (Studi Kasus di Polda Metro Jaya)." Universitas Jenderal Soedirman, 2022.
- Indriany, Khalissa Aliya. "Upaya Penanggulangan Tindak Pidana Pelecehan Seksual Anak di Media Sosial (Studi di Kepolisian Daerah Polda Metro Jaya)." *Inovasi Pembangunan: Jurnal Kelitbangan* 11, no. 01 (2023): 87.
- Maharani, Tsarina. "Kasus Penipuan Binomo: Indra Kenz Jadi Tersangka, Doni Salmanan Dilaporkan." *Retrieved Maret 21 (2022): 2022.*
- Maskun, S H. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media, 2022.
- Mumin, U Abdullah. "The Role of Information Technology in Education World (Peran Teknologi Informasi Dalam Bidang Pendidikan; E-education)." *Al-Afkar, Journal for Islamic Studies*, 2019, 104–19.
- Polri, Pusiknas Bareskrim. "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat." *Pusiknas. Polri. Go. Id. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat*, 2022.
- Prasetyo, Prasetyo, dan Mukhtar Zuhdy. "Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, no. 2 (2020): 79–88.
- Ramadhona, Herio. "Penggunaan Platform Aplikasi Only Fans untuk Cyber-Pornografi (Study Kasus Deaonly Fans di Polda Metro Jaya)." *Jurnal Impresi Indonesia* 1, no. 10 (2022): 1102–8.
- Rizkia, Nanda Dwi, dan Hardi Fardiansyah. "Metode Penelitian Hukum (Normatif dan Empiris)," 2023.
- Sembiring, Ruth Gladys, Madiasa Ablisar, Mahmud Mulyadi, dan Jelly Leviza. "Penegakan Hukum Cybercrime di Wilayah Hukum Kepolisian Daerah Sumatera Utara." *Locus Journal of Academic Literature Review*, 2023, 292–304.
- Sondakh, Jeremy Samuel Pangkey. "Pemberlakuan Ketentuan Pidana Dalam Pasal 27 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Lex Privatum* 9, no. 5 (2021).
- Sutrisno, Bambang, dan F X Bhirawa Braja Paksa. "Penegakan Hukum Terhadap Tindak Pidana Pencemaran Nama Baik Menurut Pasal 27 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Uu Iti)." *Mizan: Jurnal Ilmu Hukum* 8, no. 1 (2019): 20–26.
- Syavira, Alyfia. "Analisis Perlindungan Hukum Terhadap Korban Kejahatan Doxing (Studi pada Polda Metro Jaya)," 2022.