

KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN PENANGGULANGANNYA DALAM SISTEM HUKUM INDONESIA

Maria Hilary Paula Osintha Joni¹, Eugenia Soares De Yesus², Maria Cornelia Esparance Fallo³, Kolumbanus Antoin⁴, Marchos S.Y Sanam⁵, Yohanes Lorensio Mbale⁶

jonipaula4@gmail.com¹, eugedesoares@gmail.com², falloalice@gmail.com³,
antoinumbu9@gmail.com⁴, stefanjulio45@gmail.com⁵, yohanesmbale75@gmail.com⁶

Universitas Katolik Widya Mandira Kupang

ABSTRAK

Perkembangan teknologi informasi yang pesat membawa dampak positif sekaligus negatif bagi masyarakat. Salah satu dampak negatif yang paling signifikan adalah munculnya kejahatan siber atau cyber crime yang kian marak terjadi di Indonesia. Penelitian ini bertujuan untuk mengkaji bentuk-bentuk kejahatan teknologi informasi yang terjadi di Indonesia, menganalisis regulasi hukum yang mengatur penanggulangan cyber crime, serta mengevaluasi efektivitas penegakan hukum terhadap pelaku kejahatan siber. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Hasil penelitian menunjukkan bahwa Indonesia telah memiliki perangkat hukum yang cukup komprehensif dalam mengatur cyber crime, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya melalui UU No. 19 Tahun 2016. Namun demikian, penegakan hukum masih menghadapi berbagai kendala, antara lain keterbatasan sumber daya manusia di bidang digital forensik, lambatnya adaptasi regulasi terhadap perkembangan teknologi, serta tantangan yurisdiksi lintas negara. Penelitian ini merekomendasikan penguatan kelembagaan, peningkatan kapasitas aparat penegak hukum, dan harmonisasi regulasi internasional sebagai langkah strategis penanggulangan cyber crime di Indonesia.

Kata Kunci: Cyber Crime, Hukum Informasi Dan Transaksi Elektronik, Penegakan Hukum, Sistem Hukum Indonesia.

ABSTRACT

The rapid development of information technology has brought both positive and negative impacts to society. One of the most significant negative impacts is the increasing prevalence of cyber crime in Indonesia. This study aims to examine the forms of information technology crimes occurring in Indonesia, analyze the legal regulations governing cyber crime prevention, and evaluate the effectiveness of law enforcement against cyber crime perpetrators. The research method employed is normative legal research using the statute approach and conceptual approach. The results indicate that Indonesia already has a comprehensive legal framework regulating cyber crime, namely Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) as amended by Law No. 19 of 2016. However, law enforcement still faces various obstacles, including limited human resources in digital forensics, slow regulatory adaptation to technological developments, and cross-border jurisdictional challenges. This study recommends institutional strengthening, capacity building of law enforcement officers, and harmonization of international regulations as strategic measures for cyber crime prevention in Indonesia.

Keywords: Cyber Crime, Electronic Information And Transaction Law, Law Enforcement, Indonesian Legal System.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang begitu pesat pada era globalisasi ini telah membawa perubahan yang sangat mendasar dalam berbagai aspek kehidupan manusia. Internet sebagai medium komunikasi global tidak hanya mempercepat arus informasi, tetapi juga membuka peluang baru di bidang ekonomi, pendidikan, pemerintahan, dan sosial budaya. Menurut data Asosiasi Penyelenggara Jasa Internet

Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2023 telah mencapai lebih dari 215 juta jiwa atau sekitar 78,19 persen dari total populasi penduduk Indonesia.¹

Namun di balik manfaat yang begitu besar tersebut, perkembangan teknologi informasi juga membuka celah bagi munculnya berbagai bentuk kejahatan baru yang memanfaatkan sistem komputer dan jaringan internet sebagai sarana maupun sasaran kejahatan. Kejahatan dalam dunia siber atau yang lazim disebut cyber crime telah berkembang menjadi ancaman serius bagi keamanan nasional, stabilitas perekonomian, dan perlindungan hak-hak warga negara. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sepanjang tahun 2022, Indonesia mengalami lebih dari 2.200 serangan siber yang ditangani secara resmi, dengan kerugian yang diperkirakan mencapai triliunan rupiah.²

Realitas tersebut menuntut hadirnya kerangka hukum yang memadai untuk menanggulangi kejahatan siber secara efektif. Indonesia telah merespons tantangan ini dengan mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016. Meskipun demikian, perkembangan modus kejahatan siber yang senantiasa berevolusi mengikuti kemajuan teknologi menimbulkan pertanyaan mendasar mengenai kecukupan dan efektivitas regulasi yang ada.

Berdasarkan latar belakang tersebut, penelitian ini merumuskan tiga permasalahan pokok: (1) Apa saja bentuk-bentuk kejahatan teknologi informasi yang berkembang di Indonesia?; (2) Bagaimana pengaturan hukum positif Indonesia dalam menanggulangi cyber crime?; dan (3) Apa saja kendala yang dihadapi dalam penegakan hukum terhadap pelaku cyber crime dan bagaimana solusinya? Tujuan penelitian ini adalah memberikan gambaran komprehensif mengenai fenomena cyber crime di Indonesia sekaligus menawarkan rekomendasi kebijakan yang relevan.

METODOLOGI

Penelitian ini menggunakan metode penelitian hukum normatif (*normative legal research*), yakni penelitian yang difokuskan untuk mengkaji penerapan kaidah-kaidah atau norma-norma dalam hukum positif. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) yang mengkaji seluruh regulasi yang berkaitan dengan cyber crime, serta pendekatan konseptual (*conceptual approach*) yang merujuk pada pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum.

Bahan hukum yang digunakan terdiri dari: (1) bahan hukum primer, meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Pidana (KUHP), UU No. 11 Tahun 2008 tentang ITE beserta perubahannya, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta berbagai peraturan perundang-undangan terkait lainnya; (2) bahan hukum sekunder, berupa literatur hukum, jurnal ilmiah, hasil penelitian terdahulu, serta dokumen-dokumen resmi dari instansi terkait seperti Kepolisian Negara Republik Indonesia, Kejaksaan Agung, dan BSSN; dan (3) bahan hukum tersier, berupa kamus hukum dan ensiklopedia.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*). Analisis bahan hukum menggunakan teknik deskriptif-analitis, yakni dengan mendeskripsikan secara sistematis bahan hukum yang telah dikumpulkan, kemudian menganalisisnya secara mendalam untuk menjawab permasalahan penelitian.

¹ Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Laporan Survei Penetrasi Internet Indonesia 2023.

² Badan Siber dan Sandi Negara, *Laporan Tahunan Keamanan Siber Nasional 2022* (Jakarta: BSSN, 2023).

HASIL DAN PEMBAHASAN

A. Bentuk-Bentuk Kejahatan Teknologi Informasi di Indonesia

Kejahatan teknologi informasi atau cyber crime dapat didefinisikan sebagai setiap perbuatan yang dilarang oleh hukum pidana yang melibatkan pengetahuan teknologi komputer untuk pelaksanaannya, investigasi, atau penuntutannya (Siswanto Sunarso, 2009).³ Berdasarkan kajian terhadap kasus-kasus yang ditangani oleh Direktorat Tindak Pidana Siber Bareskrim Polri, dapat diidentifikasi beberapa bentuk cyber crime yang dominan terjadi di Indonesia:

Pertama, penipuan online (online fraud). Kejahatan ini merupakan yang paling sering dilaporkan di Indonesia. Modusnya antara lain penipuan jual beli online, phishing (pemalsuan identitas lembaga keuangan untuk mencuri data nasabah), social engineering, hingga penipuan berkedok investasi atau lowongan kerja. Data Bareskrim Polri menunjukkan bahwa kasus penipuan siber meningkat rata-rata 30 persen per tahun dalam kurun waktu 2019-2023.⁴

Kedua, penyebaran konten ilegal. Termasuk dalam kategori ini adalah penyebaran konten pornografi, hoaks (berita bohong), ujaran kebencian (hate speech), dan konten yang mengandung SARA. Kasus ini kerap mengancam kerukunan sosial dan stabilitas nasional, terutama menjelang event politik seperti pemilu dan pilkada.

Ketiga, unauthorized access dan hacking. Tindakan memasuki sistem komputer atau jaringan tanpa izin pemiliknya, baik bertujuan untuk mencuri data, merusak sistem, maupun memata-matai aktivitas pengguna. Beberapa kasus besar yang pernah terjadi di Indonesia antara lain pembobolan data BPJS Kesehatan pada tahun 2021 yang mengakibatkan bocornya data pribadi ratusan juta warga negara.⁵

Keempat, ransomware dan serangan siber terhadap infrastruktur kritis. Serangan ransomware yang mengenkripsi data korban dan meminta tebusan semakin marak terjadi dan mengancam sektor perbankan, kesehatan, dan layanan publik. Insiden serangan siber terhadap Pusat Data Nasional Sementara (PDNS) pada tahun 2024 menjadi alarm keras bagi kesiapsiagaan keamanan siber nasional.⁶

Kelima, kejahatan terhadap hak kekayaan intelektual. Pembajakan software, penyebaran konten bajakan, dan pelanggaran hak cipta melalui platform digital menjadi masalah yang belum terselesaikan secara tuntas, meskipun regulasi telah mengatur hal tersebut.

B. Pengaturan Hukum Positif Indonesia terhadap Cyber Crime

Indonesia telah memiliki sejumlah instrumen hukum untuk menanggulangi cyber crime. Instrumen utama adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE mengatur berbagai aspek transaksi elektronik dan tindak pidana siber dalam 54 pasal, termasuk larangan distribusi konten ilegal (Pasal 27-29), akses ilegal (Pasal 30), intersepsi ilegal (Pasal 31), gangguan sistem (Pasal 33), dan penyalahgunaan perangkat (Pasal 34).

³ Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari* (Jakarta: Rineka Cipta, 2009).

⁴ Data internal Direktorat Tindak Pidana Siber (Dittipidsiber), Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim Polri), periode 2019–2023.

⁵ Insiden kebocoran data peserta BPJS Kesehatan tahun 2021 yang sempat diperjualbelikan di forum daring dan menjadi perhatian publik serta Kementerian Komunikasi dan Informatika.

⁶ Insiden serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024 yang mengganggu sejumlah layanan publik dan keimigrasian secara nasional.

Selain UU ITE, terdapat beberapa regulasi pendukung lainnya, yaitu: (1) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mengatur standar keamanan sistem elektronik; (2) Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital; (3) Peraturan Menteri Komunikasi dan Informatika terkait penanganan konten negatif; serta (4) ketentuan-ketentuan dalam KUHP yang dapat diterapkan secara komplementer, seperti Pasal 362 (pencurian data), Pasal 378 (penipuan), dan Pasal 406 (perusakan).

Secara kelembagaan, penanganan cyber crime melibatkan berbagai instansi, yakni Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri sebagai ujung tombak penegakan hukum, BSSN sebagai badan yang bertanggung jawab atas keamanan siber nasional, Kementerian Komunikasi dan Informatika yang berwenang memblokir konten negatif, serta Tim Koordinasi Nasional Penanganan Informasi Berbahaya. Kerja sama antar lembaga ini diatur dalam berbagai nota kesepahaman (MoU) dan regulasi teknis.

Dalam Tabel 1 berikut ini disajikan ringkasan pasal-pasal utama UU ITE beserta ancaman pidananya:

Pasal	Substansi Larangan	Ancaman Pidana
Pasal 27 ayat (1)	Distribusi konten asusila/pornografi	Pidana 6 tahun / denda Rp 1 miliar
Pasal 27 ayat (3)	Pencemaran nama baik melalui ITE	Pidana 4 tahun / denda Rp 750 juta
Pasal 28 ayat (1)	Penyebaran berita bohong (hoaks)	Pidana 6 tahun / denda Rp 1 miliar
Pasal 30	Akses ilegal sistem komputer orang lain	Pidana 8 tahun / denda Rp 800 juta
Pasal 32	Perubahan/penghapusan informasi elektronik tanpa izin	Pidana 8 tahun / denda Rp 2 miliar
Pasal 35	Pemalsuan dokumen elektronik	Pidana 12 tahun / denda Rp 12 miliar

Tabel 1. Ketentuan Pidana dalam UU ITE (Sumber: UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016)

C. Kendala Penegakan Hukum dan Solusi Strategis

Meskipun kerangka regulasi telah tersedia, penegakan hukum terhadap cyber crime masih menghadapi sejumlah kendala substansial. Pertama, keterbatasan sumber daya manusia yang memiliki kompetensi di bidang digital forensik dan keamanan siber. Jumlah penyidik yang terlatih khusus menangani perkara siber masih sangat terbatas dibandingkan dengan volume perkara yang terus meningkat (Maskun, 2013).⁷ Hal ini berdampak pada lamanya proses penyidikan dan potensi hilangnya barang bukti digital yang bersifat volatile.

Kedua, persoalan yurisdiksi lintas negara (cross-border jurisdiction). Pelaku cyber crime seringkali beroperasi dari luar wilayah Indonesia dan memanfaatkan celah hukum antarnegara untuk menghindari penuntutan. Konvensi Budapest tentang Kejahatan Siber yang menjadi acuan internasional belum diratifikasi oleh Indonesia, sehingga kerja sama

⁷ Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Jakarta: Kencana Prenada Media Group, 2013).

penanganan perkara lintas yurisdiksi masih terhambat.⁸

Ketiga, lambatnya adaptasi regulasi terhadap perkembangan teknologi. UU ITE yang terakhir direvisi pada tahun 2016 dinilai sudah mulai tertinggal dari perkembangan fenomena kejahatan siber kontemporer, seperti kejahatan berbasis kecerdasan buatan (AI), deepfake, dan serangan terhadap aset kripto. Revisi UU ITE kembali dilakukan pada tahun 2024 melalui Undang-Undang Nomor 1 Tahun 2024, namun implementasinya masih memerlukan peraturan pelaksana yang komprehensif.⁹

Keempat, rendahnya literasi digital masyarakat menjadikan mereka rentan menjadi korban kejahatan siber. Edukasi kepada masyarakat mengenai keamanan digital masih sangat terbatas jangkauannya, terutama di daerah terpencil.

Terhadap kendala-kendala tersebut, beberapa solusi strategis yang dapat direkomendasikan antara lain: (1) penguatan kelembagaan dan peningkatan anggaran untuk pengembangan kapasitas aparat penegak hukum di bidang siber; (2) percepatan ratifikasi Konvensi Budapest dan penguatan kerja sama hukum timbal balik (mutual legal assistance) dengan negara-negara lain; (3) pembentukan pengadilan khusus perkara siber yang dilengkapi dengan hakim dan jaksa yang memiliki kompetensi teknis memadai; (4) penguatan ekosistem keamanan siber nasional melalui sinergi antara pemerintah, sektor swasta, akademisi, dan masyarakat; serta (5) kampanye literasi digital yang masif dan berkelanjutan.

KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat ditarik beberapa simpulan sebagai berikut. Pertama, cyber crime di Indonesia telah berkembang dalam berbagai bentuk yang semakin kompleks dan canggih, dengan penipuan online, penyebaran konten ilegal, unauthorized access, ransomware, dan pelanggaran hak kekayaan intelektual sebagai jenis yang paling dominan. Kedua, Indonesia telah memiliki kerangka hukum positif yang cukup komprehensif untuk menanggulangi cyber crime, terutama melalui UU ITE beserta sejumlah peraturan pelaksana dan regulasi sektoral terkait. Ketiga, penegakan hukum terhadap cyber crime masih menghadapi berbagai kendala serius yang bersifat struktural, kelembagaan, dan teknis, sehingga diperlukan langkah-langkah strategis yang sistematis dan berkelanjutan.

Saran

Penelitian ini merekomendasikan beberapa hal berikut: (1) pemerintah perlu segera meratifikasi Konvensi Budapest sebagai langkah akselerasi kerja sama internasional penanggulangan cyber crime; (2) perlu dilakukan peningkatan kapasitas dan kuantitas penyidik siber melalui program pendidikan dan pelatihan berkelanjutan; (3) revisi berkala terhadap UU ITE perlu dilakukan seiring perkembangan teknologi agar regulasi senantiasa relevan dan efektif; (4) penguatan koordinasi lintas lembaga dalam penanganan perkara siber perlu segera dibenahi melalui pembentukan mekanisme yang lebih terstruktur; serta (5) peningkatan literasi digital masyarakat harus menjadi prioritas nasional sebagai upaya pencegahan dini kejahatan siber.

⁸ *Convention on Cybercrime* (Konvensi Budapest), Council of Europe, ditandatangani di Budapest pada 23 November 2001; hingga kini Indonesia belum menjadi negara pihak (state party) atas konvensi ini.

⁹ Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

DAFTAR PUSTAKA

- Badan Siber dan Sandi Negara. (2023). Laporan Tahunan Keamanan Siber Nasional 2022. Jakarta: BSSN.
- Chazawi, A. (2011). Hukum Pidana Positif Penghinaan. Surabaya: PMN.
- Edmon Makarim. (2003). Kompilasi Hukum Telematika. Jakarta: RajaGrafindo Persada.
- Marzuki, P. M. (2011). Penelitian Hukum. Jakarta: Kencana Prenada Media.
- Maskun. (2013). Kejahatan Siber (Cyber Crime): Suatu Pengantar. Jakarta: Kencana Prenada Media Group.
- Moeljatno. (2008). Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.
- Ramli, A. M. (2004). Cyber Law dan HAKI dalam Sistem Hukum Indonesia. Bandung: Refika Aditama.
- Siswanto Sunarso. (2009). Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari. Jakarta: Rineka Cipta.
- Soesilo, R. (1995). Kitab Undang-Undang Hukum Pidana (KUHP) serta Komentar-Komentarnya Lengkap Pasal demi Pasal. Bogor: Politeia.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.
- Wahid, A., & Labib, M. (2005). Kejahatan Mayantara (Cyber Crime). Bandung: Refika Aditama.
- Widodo. (2009). Sistem Pidana dalam Cyber Crime: Alternatif Pencegahan dan Penanggulangan Kejahatan Berbasis Teknologi Informasi. Yogyakarta: Laksbang Mediatama.
- Zen, A. P. (2006). Panduan Bantuan Hukum di Indonesia. Jakarta: YLBHI.