TINJAUAN YURIDIS TERHADAP CYBERCRIME DAN KEAMANAN DATA DI ERA GLOBALISAS

Hara Tua Hutasoit[1], Debora[2]
haratua.hutasoit@student.uhn.ac.id[1], debora@uhn.ac.id[2]
Universitas HKBP Nommensen Medan

Abstrak: Era globalisasi ditandai dengan kemajuan teknologi informasi yang membawa dampak signifikan pada berbagai aspek kehidupan, termasuk dalam konteks hukum. Cybercrime menjadi salah satu tantangan utama, terutama terkait perlindungan keamanan data. Artikel ini bertujuan untuk menganalisis aspek yuridis dari cybercrime dan keamanan data, dengan fokus pada peraturan perundang-undangan di Indonesia serta harmonisasi hukum internasional. Kajian ini menemukan bahwa meskipun Indonesia memiliki perangkat hukum seperti UU ITE dan UU PDP, tantangan dalam penegakan hukum masih signifikan. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas penegak hukum, dan kerja sama internasional.
Kata Kunci: Cybercrime, Keamanan Data, Hukum, Globalisasi, UU ITE, UU PDP.

PENDAHULUAN

Globalisasi telah mendorong integrasi ekonomi, sosial, dan teknologi. Salah satu fenomena yang menonjol adalah meningkatnya ketergantungan pada teknologi digital, yang menciptakan peluang sekaligus ancaman baru. Salah satu ancaman tersebut adalah cybercrime, yang mencakup berbagai kejahatan seperti peretasan, pencurian identitas, hingga pelanggaran privasi data. Selain itu juga perkembangan teknologi informasi dan komunikasi di era globalisasi telah mendorong terciptanya ekonomi digital, namun di sisi lain juga meningkatkan risiko kejahatan siber (cybercrime). Kejahatan siber tidak hanya berdampak pada individu tetapi juga pada organisasi dan negara. Di Indonesia, berbagai insiden seperti phishing, data breaches, dan ransomware menunjukkan pentingnya penguatan regulasi dalam melindungi keamanan data.

Globalisasi juga telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk cara manusia berinteraksi, bertransaksi, dan mengelola informasi. Perkembangan teknologi informasi dan komunikasi telah menciptakan peluang ekonomi dan sosial yang tak terhingga, namun juga memunculkan risiko baru, salah satunya adalah cybercrime. Kejahatan ini mencakup berbagai aktivitas ilegal yang dilakukan melalui jaringan internet, seperti peretasan (hacking), pencurian identitas (identity theft), serangan ransomware, dan pelanggaran privasi data.

Di Indonesia, keberadaan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP) menjadi landasan utama dalam mengatur dan melindungi aktivitas digital. Namun, tantangan seperti lemahnya penegakan hukum dan kurangnya literasi digital masyarakat memperburuk kerentanan terhadap serangan siber. Dan lebih tepatnya indonesia telah memiliki kerangka hukum seperti UU ITE dan UU PDP, namun tantangan tetap ada, termasuk lemahnya law enforcement dan kurangnya kesadaran masyarakat tentang pentingnya melindungi data pribadi. Di sisi lain, hukum nasional perlu diselaraskan dengan standar internasional seperti Budapest Convention untuk menangani kejahatan siber yang bersifat lintas negara.

Cybercrime menjadi tantangan serius karena sifatnya yang lintas batas dan mampu menyebabkan kerugian besar, baik secara finansial maupun reputasi. Berdasarkan laporan Global Cybersecurity Index 2020 yang dirilis oleh International Telecommunication Union (ITU), ancaman siber terus meningkat seiring dengan semakin tergantungnya dunia pada teknologi digital. Dalam konteks Indonesia, kasus kebocoran data yang melibatkan perusahaan besar dan instansi pemerintah semakin menunjukkan urgensi untuk memperkuat sistem perlindungan hukum terhadap kejahatan siber.

Artikel ini bertujuan untuk meninjau aspek yuridis dari cybercrime dan keamanan data di Indonesia, serta mengeksplorasi bagaimana hukum nasional dapat beradaptasi dengan standar global untuk menghadapi ancaman di era digital. keamanan data di era globalisasi. Fokus kajian meliputi efektivitas regulasi yang ada, kendala dalam implementasinya, serta potensi harmonisasi dengan hukum internasional seperti Budapest Convention on Cybercrime. Dengan mengkaji isu ini, diharapkan dapat memberikan rekomendasi yang konstruktif untuk memperkuat perlindungan hukum dalam menghadapi ancaman siber yang semakin kompleks.

HASIL DAN PEMBAHASAN

1. Legal Framework of Cybercrime in Indonesia

Indonesia's primary regulation addressing cybercrime is the UU ITE (Law No. 11 of 2008, amended by Law No. 19 of 2016). This law includes provisions related to:

- Access without authority (Pasal 30)
- Manipulation and falsification of electronic information (Pasal 35)
- Defamation in digital platforms (Pasal 27).

Meskipun UU ITE berfungsi sebagai landasan hukum, implementasinya sering dikritik karena dianggap kurang efektif dalam menangani kasus cybercrime yang kompleks. Salah satu alasan adalah

keterbatasan kapasitas teknis penegak hukum.

2. Data Protection under UU PDP

The Personal Data Protection Law (UU PDP), enacted in 2022, represents a significant milestone in ensuring data security. It regulates:

- Rights of data subjects (hak subjek data) seperti hak akses dan penghapusan data.
- Obligations of data controllers (pengendali data) untuk melindungi data dari akses tidak sah.
- Administrative and criminal sanctions for violations.

However, implementation challenges include:

- Lack of technical infrastructure to support robust data protection.
- Limited awareness among businesses and individuals about compliance requirements.

3. International Legal Standards and Harmonization

Indonesia belum menjadi bagian dari Budapest Convention on Cybercrime, sebuah standar internasional yang menyediakan kerangka kerja untuk penanganan kejahatan siber secara global. Dengan menjadi anggota, Indonesia dapat memperkuat kerja sama internasional dalam:

- Mutual legal assistance (bantuan hukum timbal balik).
- Capacity building untuk penegak hukum.
- Information sharing antara negara-negara anggota.

Harmonisasi hukum nasional dengan standar global akan membantu meningkatkan efektivitas dalam menghadapi ancaman cybercrime lintas negara.

1. Definisi dan Jenis-Jenis Cybercrime

Cybercrime adalah kejahatan yang melibatkan teknologi komputer dan jaringan, baik sebagai alat, target, maupun keduanya. Kejahatan ini mencakup berbagai tindakan yang melanggar hukum, seperti:

- Hacking: Akses ilegal ke sistem komputer atau jaringan.
- Phishing: Upaya penipuan untuk memperoleh informasi pribadi, seperti kata sandi atau nomor kartu kredit, melalui email palsu atau situs web tiruan.
- Ransomware: Malware yang mengunci atau mengenkripsi data pengguna, diikuti dengan tuntutan tebusan untuk mengembalikan akses.
- Identity theft: Pencurian identitas digital untuk melakukan penipuan atau tindakan kriminal lainnya.

Cybercrime menjadi semakin kompleks di era globalisasi karena sifatnya yang lintas batas, memerlukan pendekatan hukum yang tidak hanya lokal, tetapi juga internasional.

2. Regulasi Cybercrime di Indonesia

Indonesia telah mengatur kejahatan siber melalui beberapa undang-undang, terutama Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Berikut poin-poin penting terkait cybercrime dalam UU ITE:

- Pasal 27-30: Mengatur larangan penyebaran konten negatif, akses ilegal, dan manipulasi data elektronik.
- Pasal 45: Memberikan sanksi pidana untuk pelanggaran yang diatur dalam UU ITE, dengan hukuman maksimal 12 tahun penjara atau denda hingga Rp 12 miliar.

Meski regulasi sudah ada, implementasinya sering menghadapi tantangan, seperti:

- Keterbatasan kemampuan teknis penegak hukum dalam menangani bukti digital.
- Masalah interpretasi pasal tertentu yang sering menimbulkan kontroversi, seperti Pasal 27 tentang pencemaran nama baik.

4. Keamanan Data di Era Digital

Keamanan data menjadi isu sentral di era globalisasi karena meningkatnya kasus kebocoran data. Untuk mengatasi hal ini, Indonesia mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022. UU ini mengatur:

- Hak subjek data, termasuk hak akses, penghapusan, dan perbaikan data pribadi.
- Kewajiban pengendali data untuk melindungi data dari akses tidak sah atau kebocoran.
- Sanksi administratif dan pidana bagi pelanggar.

Namun, implementasi UU PDP masih menghadapi kendala:

1. Kurangnya pemahaman masyarakat tentang hak-hak mereka terkait data pribadi.
2. Ketiadaan infrastruktur teknis yang memadai untuk mendukung penerapan regulasi.
3. Sulitnya menangani pelanggaran data yang melibatkan entitas lintas negara.
4. Harmonisasi Hukum Nasional dengan Standar Internasional

Cybercrime bersifat lintas batas, sehingga memerlukan kerja sama internasional untuk penanganannya. Standar internasional seperti Budapest Convention on Cybercrime menjadi acuan utama dalam menangani kejahatan siber. Meskipun Indonesia belum menjadi anggota konvensi ini, negara dapat mengadopsi prinsip-prinsipnya, seperti:

1. Mutual Legal Assistance (MLA) untuk memfasilitasi penyelidikan dan penuntutan lintas negara.
2. Standar minimum dalam penyimpanan dan pertukaran bukti digital.
3. Penguatan kapasitas penegak hukum dalam bidang digital forensic.
4. Tantangan dan Peluang di Era Globalisasi

Tantangan dalam mengatasi cybercrime dan menjaga keamanan data meliputi:

- Kurangnya literasi digital masyarakat, yang meningkatkan kerentanan terhadap kejahatan siber.
- Kompleksitas hukum internasional yang mempersulit penanganan kasus lintas batas.
- Ketergantungan yang tinggi pada infrastruktur digital yang rentan terhadap serangan.

Namun, globalisasi juga membuka peluang:

- Kemajuan teknologi memungkinkan pengembangan sistem keamanan yang lebih canggih.
- Kerja sama internasional, seperti forum ASEAN Cyber Capacity, memberikan platform untuk berbagi pengalaman dan strategi.

KESIMPULAN

Cybercrime dan keamanan data adalah isu hukum yang kompleks di era globalisasi. Indonesia telah menunjukkan kemajuan melalui UU ITE dan UU PDP, namun tantangan implementasi dan harmonisasi hukum internasional masih signifikan. Penguatan kapasitas teknis penegak hukum, peningkatan literasi digital masyarakat, dan kerja sama internasional menjadi prioritas untuk menghadapi ancaman ini.

DAFTAR PUSTAKA

Buku

M. Zaki, Keamanan Data dan Kejahatan Siber (Jakarta: Penerbit Pradipta, 2019), hlm. 70.

Fahmi R. dan I. Nur, Keamanan Informasi di Dunia Digital (Bandung: Penerbit Mandiri, 2020), hlm. 110.

Peraturan Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Jurnal

Nasiopoulos, G. (2019). Globalization and Technology: The Impact on Society and the Economy. Oxford University Press.

Castells, M. (2010). The Rise of the Network Society. Wiley-Blackwell.

Saini, P. (2017). Cybersecurity and Cybercrime: The Evolving Threats. Cambridge University Press, hlm. 128.

Suryana, Y. (2018). Cyber Law and Cybercrime in Indonesia. Kencana, hlm. 115.
Suyanto, T. (2023). Hukum Perlindungan Data Pribadi di Indonesia: Implementasi dan Tantangan. Penerbit Citra Aditya Bakti, hlm. 178.
Gillespie, A. (2017). Cybercrime and the Law: A Guide for Practitioners. Routledge, hlm. 235.
Wall, D. S. (2017). Cybercrime: The Transformation of Crime in the Information Age. Polity Press, hlm. 58.
Adhiatma, A. (2019). Hukum Siber di Indonesia: Implementasi dan Tantangan. Penerbit Universitas Indonesia, hlm. 134.
Brenner, S. W. (2018). Cybercrime: Criminal Threats from Cyberspace. Praeger Security International, hlm. 150.