Jurnal Kolaboratif Sains, Volume 8 No. 1, Januari 2025, 506-511

Jurnal Kolaboratif Sains
e-ISSN : 2623-2022

Homepage Journal: https://jurnal.unismuhpalu.ac.id/index.php/JKS

Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya (Desember 2024)

Cybercrime: Criminal Law Challenges in Tackling Cybercrime (December 2024)

Karolus Charlaes Bego[1*], Fajar Rahmat Aziz[2], Riadi Asra Rahmad[3], Sunarto[4], Heri Budianto[5]
[1]Universitas Flores
[2]Universitas Muhammadiyah Makassar
[3]Universitas Islam Riau
[4]Universitas 17 Agustus 1945 Semarang
[5]MAN Sumenep

***Corresponding Author**: **E-mail:** charlaes041168@gmail.com

Artikel Penelitian

Article History:
Received: 18 Nov, 2024
Revised: 21 Dec, 2024
Accepted: 29 Jan, 2025

Kata Kunci:
Cybercrime, Hukum Pidana, Kejahatan Dunia Maya, Teknologi Informasi, Tantangan Hukum

Keywords:
Cybercrime, Criminal Law, Cyber Crimes, Information Technology, Legal Challenges

DOI: 10.56338/jks.v8i1.6740

ABSTRAK

Cybercrime, atau yang lebih dikenal sebagai cybercrime, telah menjadi masalah yang semakin kompleks di seluruh dunia seiring dengan pesatnya kemajuan teknologi informasi dan komunikasi. Jaringan internet memungkinkan berbagai jenis kejahatan yang sebelumnya terbatas pada ruang fisik untuk dilakukan dengan mudah. Cybercrime mencakup berbagai jenis kejahatan, seperti peretasan, penipuan elektronik, penyebaran konten ilegal, dan kerusakan infrastruktur penting negara. Seringkali, sistem hukum pidana Indonesia saat ini tidak dapat mengikuti perkembangan cepat teknologi ini. Tujuan dari artikel ini adalah untuk menyelidiki tantangan hukum pidana yang dihadapi Indonesia dalam menangani kejahatan di dunia maya dan menawarkan solusi untuk meningkatkan kemampuan penanggulangan kejahatan di dunia maya.

ABSTRACT

Cybercrime, or better known as cybercrime, has become an increasingly complex problem around the world along with the rapid advancement of information and communication technology. The internet network allows various types of crimes that were previously limited to physical space to be committed easily. Cybercrime includes various types of crimes, such as hacking, electronic fraud, dissemination of illegal content, and damage to the country's critical infrastructure. Often, Indonesia's current criminal law system is unable to keep up with the rapid development of this technology. The purpose of this article is to investigate the criminal law challenges Indonesia faces in addressing cybercrime and offer solutions to improve its cybercrime response capabilities.

PENDAHULUAN

Kehidupan manusia telah sangat diubah oleh kemajuan pesat dalam teknologi informasi dan komunikasi. Sekarang, internet dan jaringan digital menjadi bagian integral dari hampir setiap aspek kehidupan kita, termasuk komunikasi, pendidikan, ekonomi, dan pemerintahan. Meskipun teknologi ini

memiliki banyak keuntungan, itu juga memiliki banyak masalah, terutama dalam hal kejahatan dunia maya atau cybercrime. Cybercrime tidak hanya merugikan orang atau bisnis, tetapi juga dapat mengancam keamanan nasional negara.

Kejahatan dunia maya, juga dikenal sebagai cybercrime, merujuk pada segala bentuk kejahatan yang menggunakan teknologi informasi sebagai alat atau sarana untuk melakukannya. Berbagai jenis kejahatan ini termasuk pencurian data pribadi, penipuan online, peretasan sistem komputer, dan serangan terhadap infrastruktur penting negara. Kejahatan dunia maya telah meningkat pesat dalam beberapa tahun terakhir sebagai akibat dari akses internet yang semakin mudah dan teknologi yang digunakan oleh pelaku kejahatan.

Kejahatan dunia maya telah menjadi masalah besar di Indonesia, terutama dengan meningkatnya jumlah kasus yang berkaitan dengan teknologi. Meskipun negara ini sudah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur kejahatan dunia maya, penanggulangan kejahatan dunia maya masih menghadapi banyak masalah. Sifat cybercrime yang terus berkembang seiring dengan perkembangan teknologi itu sendiri adalah salah satu masalah terbesar. Karena kejahatan dunia maya bersifat global, mereka tidak terbatas pada satu negara atau wilayah. Oleh karena itu, masalah penegakan hukum yang berkaitan dengan kejahatan cyber menjadi semakin kompleks.

Selain itu, fungsi aparat penegak hukum sangat terbatas dalam menangani kejahatan dunia maya. Banyak aparat penegak hukum di Indonesia tidak mahir dalam teknologi digital, yang membuat mereka sulit menyelidiki dan menangani kasus-kasus cybercrime. Akibatnya, untuk mengatasi masalah ini dan meningkatkan upaya penanggulangan cybercrime di Indonesia, dibutuhkan upaya keras dari berbagai pihak.

Artikel ini akan membahas lebih lanjut tentang masalah hukum pidana dalam penanggulangan kejahatan dunia maya, terutama dengan membahas peraturan perundang-undangan yang ada, tantangan penegakan hukum, dan solusi untuk meningkatkan penanggulangan kejahatan dunia maya.

METODE PENELITIAN

Data yang dikumpulkan melalui studi pustaka digunakan dalam pendekatan deskriptif analitis dalam penelitian ini. Data yang digunakan dalam penelitian ini diperoleh dari berbagai literatur yang relevan, seperti buku, jurnal, artikel, dan peraturan perundang-undangan yang berkaitan dengan masalah penegakan hukum dan cybercrime di Indonesia. Metode ini bertujuan untuk memperoleh pemahaman yang lebih mendalam tentang kesulitan yang dihadapi sistem hukum pidana Indonesia dalam menangani kasus cybercrime dan menemukan solusi yang dapat diterapkan.

HASIL DAN PEMBAHASAN

Definisi dan Jenis-jenis Cybercrime

Cybercrime, juga dikenal sebagai kejahatan dunia maya, merujuk pada segala bentuk aktivitas kriminal yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi (TIK), khususnya internet, sebagai sarana utama. Kejahatan dunia maya semakin beragam seiring perkembangan teknologi dan dapat memanfaatkan setiap celah dalam sistem digital untuk tujuan ilegal. Kejahatan ini tidak hanya merugikan orang-orang, tetapi juga dapat mengancam keamanan negara dan integritas ekonomi global. Berikut adalah beberapa jenis cybercrime utama yang semakin populer:

Hacking (Peretasan): Peretasan adalah salah satu jenis cybercrime yang paling umum dan biasanya dilakukan oleh individu atau kelompok yang sangat mahir dalam teknologi. Hacking adalah

tindakan ilegal untuk mendapatkan akses ke sistem atau jaringan dengan berbagai tujuan, seperti mencuri data pribadi, merusak sistem, atau mendapatkan akses ke informasi sensitif yang tidak seharusnya diketahui. Peretas biasanya berusaha mengeksploitasi celah dalam sistem atau perangkat lunak untuk mendapatkan akses yang tidak sah. Peretasan juga bisa terjadi pada institusi besar, lembaga pemerintahan, atau perusahaan yang menyimpan data sensitif pada skala yang lebih besar.

Penipuan Elektronik (Fraud Online) adalah penipuan yang dilakukan dengan memanfaatkan teknologi internet untuk menipu korban. Penipuan jenis ini sangat beragam, mulai dari penipuan e-commerce hingga investasi bodong dan menyamar sebagai orang atau perusahaan yang dapat dipercaya untuk menipu korban. Pelaku penipuan biasanya menggunakan situs web palsu, email phishing, atau aplikasi mobile untuk mencuri informasi pribadi atau uang korban. Penipuan ini meningkat karena transaksi digital yang cepat dan ketergantungan masyarakat terhadap internet dalam kehidupan sehari-hari.

Salah satu jenis cybercrime yang sangat meresahkan adalah pencurian identitas atau pencurian data pribadi. Mereka biasanya mencuri data pribadi seperti nomor KTP, nomor kartu kredit, informasi perbankan, atau informasi sensitif lainnya. Data yang dicuri kemudian digunakan untuk melakukan transaksi yang melanggar hukum atau penipuan. Pencurian identitas dapat terjadi dengan berbagai cara, seperti serangan phishing, penerapan malware pada perangkat korban, atau penggunaan teknik sosial engineering untuk mengelabui korban untuk memberikan informasi pribadi mereka.

Serangan terhadap Infrastruktur Vital (Critical Infrastructure Attacks) Serangan terhadap infrastruktur vital adalah jenis kejahatan dunia maya yang menyasar sektor-sektor penting yang mendukung kelangsungan hidup suatu negara, seperti sistem perbankan, sektor energi, transportasi, dan pertahanan. Serangan terhadap sektor-sektor ini bisa memiliki dampak yang sangat besar, seperti menghentikan operasional sistem perbankan yang dapat menyebabkan kerugian finansial, merusak sistem energi yang mengganggu pasokan listrik, atau bahkan merusak sistem pertahanan yang vital bagi keamanan negara. Serangan seperti ini biasanya dilakukan oleh kelompok terorganisir yang ingin merusak stabilitas negara atau mendapatkan keuntungan finansial.

Penyebaran Konten Ilegal adalah salah satu jenis kejahatan dunia maya yang paling berbahaya bagi masyarakat. Konten yang disebarkan dapat berupa ujaran kebencian, pornografi anak, hoaks, atau konten yang melanggar hak cipta. Penyebaran konten yang melanggar hukum dapat menyebabkan ketegangan sosial, gangguan psikologis pada korban, atau bahkan tindak kekerasan. Karena pelaku dapat menyembunyikan identitas mereka melalui teknologi seperti VPN atau penggunaan jaringan anonim seperti Tor, kejahatan ini seringkali sulit dilacak.

Tantangan Hukum Pidana dalam Menanggulangi Cybercrime

Penegakan hukum kejahatan dunia maya di Indonesia menghadapi banyak tantangan yang sulit diatasi karena kejahatan dunia maya terus berkembang dan dinamis. Beberapa tantangan utama yang dihadapi dalam penanggulangan kejahatan dunia maya antara lain:

Kurangnya Peraturan yang Memadai: Meskipun Indonesia memiliki Undang-Undang Informasi dan Transaksi Elektronik (ITE) yang dimaksudkan untuk mengontrol aktivitas dunia maya, undang-undang tersebut sering dianggap tidak efektif dalam memerangi berbagai bentuk cybercrime yang semakin kompleks. UU ITE, yang disahkan pada tahun 2008, bertujuan untuk mengawasi transaksi elektronik dan melindungi data pribadi. Namun, undang-undang tersebut tidak sepenuhnya mengantisipasi kemajuan pesat dalam teknologi digital, seperti penggunaan blockchain, cryptocurrency, dan kecerdasan buatan (AI). Peraturan saat ini perlu diperbarui untuk menangani jenis cybercrime baru yang memanfaatkan teknologi canggih ini.

Pengumpulan Bukti Digital yang Rumit: Pengumpulan dan penyelidikan bukti digital dalam kasus cybercrime juga merupakan masalah yang signifikan. Data yang tersimpan di perangkat komputer, server, atau cloud seringkali merupakan informasi penting dalam penyidikan, tetapi dapat dengan mudah diubah atau dihapus. Selain itu, bukti digital biasanya tersebar di banyak tempat di dalam

dan luar negeri, membuat pengumpulan bukti lebih sulit. Untuk menangani bukti elektronik ini secara sah dan efisien, penegak hukum membutuhkan perangkat forensik digital yang sangat canggih serta keterampilan teknis yang tinggi.

Sifat Cybercrime yang Lintas Negara: Sifat ini adalah lintas negara. Pelaku kejahatan dunia maya biasanya beroperasi dari luar negeri, yang membuat penegakan hukum di Indonesia sangat sulit. Ini membutuhkan kerja sama global yang lebih erat. Selain itu, perbedaan peraturan hukum di setiap negara sering menghambat proses ekstradisi pelaku cybercrime yang berada di luar negeri. Oleh karena itu, diperlukan mekanisme yang lebih efektif di tingkat internasional untuk memerangi kejahatan dunia maya yang mencakup lebih dari satu negara.

Keterbatasan Sumber Daya Manusia dan Infrastruktur: Kekurangan sumber daya manusia yang terlatih di bidang teknologi digital dan forensik komputer terus menjadi kendala yang signifikan bagi upaya Indonesia untuk memerangi cybercrime. Banyak penegak hukum tidak memiliki kemampuan untuk menangani kasus cybercrime yang kompleks. Selain itu, infrastruktur yang ada saat ini masih terbatas. Ini termasuk sistem pelacakan kejahatan dunia maya dan laboratorium forensik digital. Hal ini menyebabkan proses penanganan kasus kejahatan internet menjadi lebih lama dan tidak efisien.

Peran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Beberapa aspek penting dari UU ITE dalam kaitannya dengan kejahatan dunia maya antara lain: UU ITE memberikan dasar hukum untuk berbagai hal, mulai dari transaksi digital, komunikasi melalui media elektronik, hingga penanggulangan berbagai bentuk kejahatan dunia maya:

Regulasi Transaksi Elektronik UU ITE mengatur berbagai jenis transaksi elektronik, seperti jual beli, perjanjian elektronik, dan tanda tangan digital. Regulasi ini memberikan perlindungan hukum yang sah untuk transaksi di internet, yang meningkatkan kepercayaan masyarakat terhadap transaksi melalui platform digital.

Penyalahgunaan Teknologi Informasi: UU ITE mengatur penyalahgunaan teknologi informasi seperti peretasan, penyebaran konten ilegal, penipuan online, dan pencurian identitas. Tujuan dari hukuman yang diatur dalam UU ITE adalah untuk memberikan efek jera kepada pelaku kejahatan dunia maya. Namun, dengan adanya kemajuan teknologi baru, UU ITE harus diperbarui untuk mengantisipasi pelanggaran cyber yang semakin kompleks.

Penyelesaian Sengketa dan Perlindungan Data Pribadi: UU ITE juga mengatur penyelesaian sengketa terkait transaksi elektronik dan perlindungan data pribadi. Dalam hal ini, masyarakat dapat menuntut ganti rugi jika mereka menjadi korban penipuan atau kejahatan dunia maya lainnya, menurut UU ITE. Selain itu, perlindungan data pribadi yang dijamin oleh UU ITE dapat membantu mencegah pihak yang tidak bertanggung jawab mengambil data pribadi Anda.

Strategi Penanggulangan Cybercrime di Indonesia

Indonesia perlu mengambil tindakan strategis yang mencakup berbagai hal, mulai dari pembaruan regulasi hingga pemberdayaan masyarakat dan aparat penegak hukum untuk menangani cybercrime secara efektif. Beberapa langkah penting yang harus dilakukan termasuk:

Pembaruan dan Penyempurnaan Peraturan ITE: Pembaruan peraturan ITE sangat penting untuk memastikan bahwa peraturan ini dapat beradaptasi dengan kemajuan teknologi yang begitu pesat. Perubahan ini harus mencakup pengaturan terhadap jenis cybercrime baru yang muncul, seperti blockchain, cryptocurrency, dan AI. Selain itu, prosedur penyidikan dan pengumpulan bukti elektronik

harus diperbarui untuk lebih sesuai dengan masalah yang ada.

Peningkatan Kapasitas Penegak Hukum: Polisi, jaksa, dan hakim harus dilatih lebih lanjut tentang teknologi digital, forensik komputer, dan prosedur penanganan bukti elektronik. Selain itu, penegak hukum harus dibekali dengan peralatan forensik digital yang lebih canggih untuk menangani kasus cybercrime dengan lebih baik. Pelatihan ini akan membuat mereka siap untuk menangani kasus cybercrime yang semakin kompleks.

Kerja Sama Internasional dalam Penanggulangan Cybercrime: Karena cybercrime lintas negara, kerja sama internasional sangat penting untuk memeranginya. Untuk mempercepat proses penyelidikan dan pertukaran informasi terkait pelaku cybercrime, Indonesia harus memperkuat hubungannya dengan negara lain. Kerja sama ini dapat mencakup penyidikan bersama, berbagi data bukti digital, dan proses ekstradisi pelaku yang berada di luar negeri.

Edukasi dan Kesadaran Masyarakat: Salah satu langkah pencegahan yang paling efektif adalah memberi tahu orang-orang tentang pentingnya menjaga data pribadi dan berhati-hati saat berinteraksi di internet. Pemerintah dapat meminta organisasi non-pemerintah untuk mengadakan kampanye pendidikan yang membahas berbagai jenis kejahatan internet, cara menghindarinya, dan bagaimana melindungi data pribadi saat berada di internet. Edukasi ini sangat penting untuk membentuk pola tindakan yang konsisten.

KESIMPULAN

Salah satu jenis kejahatan yang semakin kompleks dan sulit diatasi di era digital ini adalah cybercrime. Beberapa masalah besar yang dihadapi oleh hukum pidana Indonesia dalam menangani cybercrime mencakup kurangnya regulasi yang memadai, kesulitan dalam pengumpulan bukti digital, dan fakta bahwa kejahatan dunia maya itu sendiri tersebar di seluruh dunia. Meskipun Indonesia memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), undang-undang tersebut harus diperbarui untuk memenuhi perkembangan teknologi yang cepat.

Indonesia harus memperkuat undang-undangnya, memperkuat sumber daya manusia penegak hukumnya, meningkatkan kerja sama dengan negara lain, dan menyelenggarakan pelatihan masyarakat untuk menghentikan kejahatan dunia maya. Langkah-langkah ini diharapkan dapat meningkatkan pengendalian cybercrime di Indonesia dan memberikan perlindungan yang lebih baik bagi masyarakat Indonesia.

DAFTAR PUSTAKA

Hafid, M., Firjatullah, F. Z., Pamungkaz, B. W., Magister, S., Hukum, I., Wijaya, U., & Surabaya, K. (2023). Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara Muhammad. Pendidikan Tambusai, 7(2), 9548–9556.

Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. Jurnal Hukum Dan HAM Wara Sains, 2(6), 517–525. https://doi.org/10.58812/jhhws.v2i6.447

Magister, P., Hukum, I., & Islam, U. (2023). Indragiri Law Review. 1(1), 19–24.

Mulasari, L. (2012). Kebijakan Formulasi Tentang Tindak Pidana Kesusilaan Di Dunia Maya Dalam Perspektif Hukum Islam. Masalah-Masalah Hukum, 41(1), 98–109. https://ejournal.undip.ac.id/index.php/mmh/article/view/4165

Safitri, W., & Fitry, A. (2023). Prosiding Seminar Nasional Penelitian dan Pengabdian kepada Masyarakat 2 Tahun 2023 dengan tema " Inovasi Penelitian dan Pengabdian kepada Masyarakat menuju Indonesia Emas 2045"

Valentine, V., Septiani, C. S., & Parshusip, J. (2024). Menghadapi Tantangan Dan Solusi Cybercrime Di Era Digital Facing Cybercrime Challenges And Solutions In The Digital Era. 1, 2–6.

Yuda, Z. A. W., Rahmasari, H., & Gunawan, T. A. (2024). Efektivitas Dan Penerapan Hukum Pidana Terhadap Cybercrime Di Indonesia. Causa: Jurnal Hukum Dan Kewarganegaraan, 4(10), 61–70.