Aurelia: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia
E-ISSN: 2964-2493 P-ISSN: 2962-0430
Vol. 4 No. 1 Januari 2025

# Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Pencegahan dan Penanganan Kasus Tindak Pidana Cyber Crime

**Oky Syalendro[1] Arief Fahmi Lubis[2] R. Yusak Andri Ende Putra[3]**
Magister Hukum Militer, Sekolah Tinggi Hukum Militer (AHM-PTHM), Kota Jakarta Timur, Provinsi Daerah Khusus Ibu Kota Jakarta, Indonesia[1,2,3]
Email: okysyalendro15@gmail.com[1]

***Abstract***

*Cybercrime refers to crimes conducted through computer networks and the internet, encompassing various illegal activities such as data theft, online fraud, hacking, and malware distribution. In Indonesia, regulations concerning cybercrime are primarily governed by Law Number 11 of 2008 on Electronic Information and Transactions (EIT Law), which was later amended by Law Number 19 of 2016. The handling of cybercrime in Indonesia has evolved alongside rapid digitalization, particularly in the financial, telecommunications, and social media sectors.This study aims to analyze the application of cybercrime laws in Indonesia and the challenges faced in law enforcement. Additionally, it examines the preventive efforts made by various stakeholders, including the government, private sector, and the public, through the strengthening of security infrastructure, digital literacy campaigns, and international collaboration in tackling cybercrime.The research methodology used in this study is normative juridical with a legislative and case study approach. The author examines various regulations, including the EIT Law and the Personal Data Protection Law, as well as notable cybercrime cases in Indonesia, such as ransomware attacks on hospitals and data theft in the banking sector.The study concludes that while Indonesia has a strong legal framework for addressing cybercrime, challenges remain in the ability of law enforcement to apply digital forensic technology, low public digital literacy, and suboptimal international cooperation. Therefore, strengthening law enforcement capacity, developing data protection policies, and increasing public awareness are necessary to address the growing cybercrime threat.*

***Keywords:*** *Cybercrime, EIT Law, Cybersecurity, Prevention, Law Enforcement*

**Abstrak**

*Cyber crime* merupakan kejahatan yang dilakukan melalui jaringan komputer dan internet, mencakup berbagai bentuk aktivitas ilegal seperti pencurian data, penipuan daring, peretasan, hingga penyebaran malware. Di Indonesia, peraturan terkait cyber crime terutama diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diamandemen dengan Undang-Undang Nomor 19 Tahun 2016. Penanganan kejahatan siber di Indonesia berkembang seiring dengan pesatnya digitalisasi, khususnya di sektor keuangan, telekomunikasi, dan media sosial. Penelitian ini bertujuan untuk menganalisis penerapan hukum cyber crime di Indonesia serta tantangan dalam penegakan hukumnya. Selain itu, penelitian ini juga mengkaji upaya pencegahan yang dilakukan oleh berbagai pihak, termasuk pemerintah, sektor swasta, dan masyarakat, melalui penguatan infrastruktur keamanan, kampanye literasi digital, serta kolaborasi internasional dalam menanggulangi kejahatan siber.Metode yang digunakan dalam penelitian ini adalah yuridis normatif dengan pendekatan perundang-undangan dan studi kasus. Penulis meneliti berbagai regulasi, termasuk Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi, serta kasus-kasus *cyber crime* yang terjadi di Indonesia, seperti serangan ransomware pada rumah sakit dan pencurian data perbankan. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki kerangka hukum yang cukup kuat untuk menangani kejahatan siber, tantangan masih ada terkait kemampuan penegak hukum dalam menerapkan teknologi forensik digital, rendahnya literasi digital masyarakat, dan kerjasama internasional yang belum optimal. Oleh karena itu, diperlukan penguatan kapasitas penegak hukum, pengembangan kebijakan perlindungan data, dan peningkatan kesadaran masyarakat untuk menghadapi ancaman kejahatan siber yang terus berkembang.

**Kata Kunci:** Cyber Crime, UU ITE, Keamanan Siber, Pencegahan, Penegakan Hukum

**PENDAHULUAN**

Dalam era digital yang semakin berkembang, teknologi informasi telah membawa dampak signifikan terhadap kehidupan masyarakat. Meskipun kemajuan ini memberikan banyak manfaat, penggunaan teknologi informasi juga memunculkan risiko baru, termasuk tindak pidana siber atau *cyber crime*. Tindak pidana ini meliputi berbagai aktivitas ilegal yang dilakukan melalui jaringan komputer atau internet, seperti pencurian data, penipuan daring (*online fraud*), peretasan, penyebaran virus, hingga pornografi anak dan terorisme siber (Lubis, 2020). Di Indonesia, peraturan mengenai *cyber crime* diatur dalam beberapa undang-undang, salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbarui dengan Undang-Undang Nomor 19 Tahun 2016. Undang-undang ini mengatur tentang berbagai aspek penggunaan teknologi informasi, termasuk sanksi pidana bagi pelaku tindak kejahatan siber (Soekanto, 2019).

Pemerintah Indonesia telah mengambil sejumlah langkah dalam upaya pencegahan dan penanganan *cyber crime*. Upaya pencegahan dilakukan melalui literasi digital, peningkatan kesadaran masyarakat akan risiko siber, serta pengembangan kerangka regulasi yang lebih ketat. Di sisi lain, penanganan kejahatan siber melibatkan berbagai instansi penegak hukum, termasuk kepolisian siber dan lembaga lain yang terkait dengan keamanan siber.Namun, meskipun telah ada peraturan yang cukup komprehensif, tantangan dalam mengatasi *cyber crime* tetap besar, terutama karena sifatnya yang lintas batas dan berkembang pesat seiring dengan inovasi teknologi. Dengan demikian, kerjasama internasional dan peningkatan kapasitas penegak hukum menjadi hal yang sangat penting dalam upaya pemberantasan tindak pidana siber di Indonesia. *Cyber crime* adalah kejahatan yang dilakukan melalui jaringan komputer dan internet. Fenomena ini menjadi perhatian global karena dampaknya yang luas, mulai dari pencurian identitas hingga serangan terhadap infrastruktur kritis. Di Indonesia, perkembangan teknologi yang pesat disertai dengan meningkatnya kasus *cyber crime* memerlukan penanganan hukum yang efektif. Saat ini, globalisasi sedang menuju era serba digital, atau dunia digital, karena kemajuan dalam teknologi informasi dan komunikasi (Shidarta, 2022). Oleh karena itu, sangat menggembirakan melihat kemajuan dunia yang rumit, beragam, dan pluralistik karena kemajuan teknologi komputer dan internet telah menjadi instrumen baru bagi negara-negara di seluruh dunia untuk digunakan sebagai alat untuk melakukan penetrasi, pengaruh, dan infiltrasi ke negara lain.Globalisasi memungkinkan negara-negara untuk berdagang secara bebas satu sama lain, menghapus kekuatan hegemonik (Putro, 2019). Upaya setiap negara untuk berkembang secara ekonomi, sosial, dan budaya menyebabkan perang ekonomi, sosial, dan budaya (Koos, 2022). Atas dasar globalisasi, pasar bebas, dan persaingan untuk menguasai sumber daya langka, konflik energi, pangan, dan air meningkat. .Baik di masa kini maupun masa depan, teknologi informasi akan menjadi sangat penting. Negara-negara di seluruh dunia berharap dapat menuai beberapa keuntungan dan peluang berkat kemajuan teknologi informasi (Widhiyanti, 2020).

Meskipun kemajuan teknologi informasi memiliki banyak dampak positif pada masyarakat, ada alasan untuk khawatir tentang potensi penyalahgunaannya (Garnett & James, 2020). karena kemajuan teknologi dapat menyebabkan aktivitas kriminal meningkat, dan karena kejahatan selalu ada dan akan terus berkembang dan mengambil bentuk baru di abad-abad mendatang. Perkembangan teknologi telah memungkinkan perubahan dan penyesuaian yang cepat dalam cara hidup yang tidak terbatas. Meluasnya teknologi ini, yang memungkinkan bisnis dan komunikasi jarak jauh, dapat dikaitkan dengan pertumbuhan ekonomi yang cepat (Fadhli & Bahri, 2020). Evolusi teknologi informasi telah membuat hal-hal yang tampaknya tidak mungkin menjadi mungkin dan membuat hal-hal yang tampaknya mustahil menjadi mungkin. Namun, kejahatan canggih seperti *cybercrime* telah muncul sebagai akibatnya,

menimbulkan kekhawatiran baru. Sejarah kejahatan dunia maya di Indonesia, terutama di industri keuangan, dapat dilacak kembali sejak tahun 1983. Pada tahun 1983, Indonesia mulai mengenal kejahatan dunia maya (*cyber crime*), yang pada awalnya masih terbatas pada kejahatan yang bersifat lokal dan sederhana. Salah satu kasus pertama yang tercatat adalah peretasan sistem komputer bank. Meskipun kejahatan ini belum terorganisir secara luas, peretasan ini membuka mata pihak berwenang dan industri keuangan mengenai potensi ancaman dari penggunaan teknologi informasi yang semakin berkembang (Bank Indonesia, 2009). Seiring dengan meningkatnya adopsi teknologi informasi di sektor keuangan selama tahun 1990an, kejahatan dunia maya mulai berkembang dengan lebih kompleks. Pada periode ini, kasus-kasus seperti pembobolan sistem perbankan dan pencurian data nasabah mulai sering terjadi. Para pelaku *cyber crime* memanfaatkan celah keamanan dalam sistem perbankan yang mulai menggunakan jaringan internet untuk transaksi dan pengolahan data.

Kasus yang signifikan pada periode ini termasuk pembobolan ATM dan pencurian identitas nasabah melalui skimming, di mana para pelaku berhasil mencuri informasi dari kartu ATM untuk mengakses rekening nasabah secara ilegal. Krisis moneter yang melanda Indonesia pada tahun 1997-1998 memperburuk kondisi keamanan di sektor keuangan. Di tengah kekacauan ekonomi, terjadi peningkatan kejahatan dunia maya, terutama di sektor perbankan. Bank-bank yang sudah lemah dari segi likuiditas dan pengawasan menjadi sasaran empuk para pelaku *cyber crime*, yang semakin canggih dalam mengeksploitasi sistem yang kurang aman. Memasuki tahun 2000an, Indonesia mulai serius menangani kejahatan dunia maya. Pihak berwenang memperkuat regulasi dan pengawasan terhadap industri keuangan, termasuk dalam hal keamanan siber. Bank Indonesia, sebagai otoritas moneter, mulai memperkenalkan kebijakan-kebijakan untuk meningkatkan keamanan sistem pembayaran dan transaksi keuangan. Pada tahun 2008, Indonesia memberlakukan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang secara khusus mengatur kejahatan dunia maya, termasuk di sektor keuangan (UU ITE, 2008). Undang-Undang ini menjadi landasan hukum dalam penanganan dan penindakan terhadap kejahatan siber di Indonesia. Dengan semakin pesatnya digitalisasi di sektor keuangan, kejahatan dunia maya pun semakin beragam dan kompleks. Fenomena seperti phishing, malware, dan ransomware menjadi tantangan utama bagi industri keuangan. Perbankan digital, yang semakin populer di kalangan masyarakat, menjadi target utama para pelaku *cyber crime*.Laporan dari Otoritas Jasa Keuangan (OJK) menunjukkan bahwa sektor keuangan, terutama perbankan dan fintech, sering menjadi sasaran serangan siber. Di era ini, kolaborasi antara pemerintah, otoritas keuangan, dan sektor swasta menjadi kunci dalam menghadapi ancaman siber yang terus berkembang (OJK, 2019).

Kejahatan dunia maya di Indonesia telah berkembang dengan berbagai bentuk seiring dengan meningkatnya penggunaan teknologi informasi dan internet. Pembajakan perangkat lunak merupakan salah satu bentuk kejahatan dunia maya yang paling awal dan paling umum di Indonesia. Pembajakan ini melibatkan penggandaan dan distribusi perangkat lunak tanpa izin dari pemilik hak cipta. Di Indonesia, praktik ini sangat umum terutama karena tingginya harga perangkat lunak asli dan rendahnya kesadaran hukum terkait hak cipta. Indonesia pernah masuk dalam daftar negara dengan tingkat pembajakan perangkat lunak tertinggi di dunia. Menurut laporan BSA (*Business Software Alliance*), pada tahun 2009, sekitar 86% dari perangkat lunak yang digunakan di Indonesia adalah hasil bajakan (BSA, 2010). Ransomware adalah jenis malware yang mengenkripsi data korban, dan pelaku kemudian meminta tebusan (*ransom*) untuk memulihkan akses data tersebut. Kejahatan ini mulai meningkat di Indonesia, terutama menyerang organisasi besar seperti rumah sakit dan perusahaan.Pada tahun 2021, sebuah rumah sakit besar di Jakarta menjadi korban serangan ransomware, yang menyebabkan gangguan besar dalam operasional dan pelayanan medis karena data pasien terenkripsi oleh

pelaku. Pembobolan enkripsi merupakan tindakan ilegal yang dilakukan untuk menembus sistem keamanan yang dilindungi oleh enkripsi, dengan tujuan untuk mengakses data atau informasi yang seharusnya terlindungi. Kejahatan ini menjadi semakin umum dengan berkembangnya transaksi digital dan penyimpanan data sensitif secara elektronik. Pada tahun 2012, terjadi kasus peretasan data pelanggan di sebuah bank besar di Indonesia, di mana pelaku berhasil menembus enkripsi keamanan dan mencuri data nasabah, termasuk informasi keuangan yang sensitif (BSSN, 2021b). Phishing adalah bentuk penipuan di mana pelaku menyamar sebagai entitas yang sah untuk mencuri informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya. Phishing sering dilakukan melalui email, media sosial, atau situs web palsu. Pada tahun 2019, ribuan nasabah bank di Indonesia menjadi korban phishing melalui email yang tampak seperti berasal dari bank mereka, yang meminta informasi login perbankan mereka. Data yang dicuri kemudian digunakan untuk mengakses rekening mereka dan mencuri uang.

Penggunaan kartu kredit curian melibatkan pencurian informasi kartu kredit, yang kemudian digunakan oleh pelaku untuk melakukan transaksi tanpa sepengetahuan pemilik kartu. Kejahatan ini meningkat seiring dengan pertumbuhan *e-commerce* di Indonesia. Pada tahun 2017, terjadi kasus besar di mana sindikat internasional berhasil mencuri data ribuan kartu kredit milik warga Indonesia melalui skimming dan phishing. Data tersebut kemudian dijual di pasar gelap (*dark web*) atau digunakan untuk transaksi online.Penipuan bank mencakup berbagai metode, termasuk phising, pengelabuan melalui email atau telepon (*vishing*), dan manipulasi sistem perbankan untuk mencuri uang dari rekening nasabah. Penipuan ini seringkali melibatkan teknologi canggih untuk mengelabui sistem keamanan perbankan.Pada tahun 2020, Otoritas Jasa Keuangan (OJK) melaporkan peningkatan signifikan dalam kasus penipuan bank di Indonesia, terutama melalui skema phising, di mana pelaku menipu nasabah untuk memberikan informasi sensitif seperti PIN dan password perbankan (OJK, 2020). Carding adalah kegiatan mencuri informasi kartu kredit dan menggunakan informasi tersebut untuk melakukan pembelian atau transaksi online. Kejahatan ini sering kali melibatkan sindikat internasional yang menjual atau membeli informasi kartu kredit curian.Pada tahun 2020, Kepolisian Indonesia berhasil menangkap beberapa pelaku carding yang berhasil meraup miliaran rupiah dengan mencuri dan menggunakan data kartu kredit milik warga negara asing.

Adapun Penyebaran konten pornografi melalui internet adalah kejahatan dunia maya yang memiliki dampak sosial yang besar di Indonesia, yang mayoritas penduduknya beragama Islam dan memiliki nilai-nilai moral yang kuat. Konten pornografi sering disebarkan melalui situs web, media sosial, dan aplikasi pesan instan. Pada tahun 2018, polisi berhasil menangkap sindikat yang mengoperasikan situs web penyebaran konten pornografi terbesar di Indonesia. Situs tersebut memiliki jutaan pengguna dan menyebarkan ribuan konten pornografi ilegal (Polisi Republik Indonesia, 2018). Kejahatan dunia maya memiliki karakteristik khusus yang membedakannya dari kejahatan konvensional, meskipun pada dasarnya semua kejahatan tersebut melibatkan pelanggaran hukum yang nyata. Berikut penjelasan rinci mengenai sifat umum kejahatan dunia maya, siapa pelakunya, dan bagaimana aktivitas dunia maya dapat diklasifikasikan sebagai tindakan hukum nyata (BSSN, 2021b):

1. Karakteristik Umum Kejahatan Dunia Maya terbagi menjadi tiga diantaranya:
   a. Akses dan Kekuasaan atas Teknologi. Kejahatan dunia maya sering dilakukan oleh individu yang memiliki pengetahuan atau akses terhadap teknologi dan internet. Ini dapat mencakup:

1) Teknisi IT dan profesional keamanan mereka yang memiliki keahlian dalam teknologi informasi dan keamanan komputer sering kali memiliki kemampuan untuk melakukan atau melindungi diri dari serangan siber.
2) Pengguna biasa dengan keterampilan teknologi dengan kemajuan teknologi, pengguna biasa pun dapat melakukan kejahatan dunia maya menggunakan perangkat lunak atau alat yang tersedia secara online.

b. Anonimitas dan Jarak. Kejahatan dunia maya memungkinkan pelaku untuk melakukan tindak kejahatan dari jarak jauh, sering kali tanpa mengungkapkan identitas mereka. Hal ini dapat mencakup penggunaan VPN, proxy, atau alat anonim lainnya untuk menyembunyikan lokasi dan identitas pelaku.
c. Lingkungan Virtual. Kejahatan dunia maya terjadi dalam ruang virtual yang berbeda dari dunia fisik. Meskipun demikian, tindakan ini tetap memiliki dampak yang nyata terhadap individu, organisasi, dan masyarakat. Misalnya, pencurian data pribadi online dapat menyebabkan kerugian finansial dan kerusakan reputasi di dunia nyata.

2. Profil pelaku kejahatan dunia maya terbiasa tidak ada profil atau rentang usia tertentu yang bisa digunakan untuk menentukan pelaku kejahatan dunia maya. Pelaku kejahatan dunia maya bisa berupa remaja dengan akses mudah ke internet dan perangkat teknologi, remaja dapat terlibat dalam kejahatan dunia maya, seperti hacking atau pembajakan perangkat lunak. Bahkan orang dewasa yang memiliki keterampilan teknis atau akses ke sumber daya dapat melakukan kejahatan yang lebih kompleks, seperti penipuan bank atau ransomware. Ataupun individu dengan keterampilan khusus mereka yang bekerja di bidang teknologi informasi atau keamanan siber juga bisa terlibat dalam kejahatan, baik secara individu atau sebagai bagian dari sindikat kriminal.

Motivasi pelaku kejahatan dunia maya sangat bervariasi, mulai dari keuntungan finansial, pembalasan pribadi, hingga sekadar tantangan teknis. Ini mencerminkan keragaman latar belakang dan tujuan pelaku. Aktivitas dunia maya, meskipun terjadi di ruang virtual, diakui dan diklasifikasikan sebagai tindakan hukum nyata. Banyak negara, termasuk Indonesia, telah memperbarui hukum mereka untuk mencakup kejahatan dunia maya. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sudah mengatur kejahatan dunia maya, termasuk penipuan online, pembajakan, dan penyebaran konten ilegal. (UU ITE, 2008) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 mengakomodasi perkembangan terbaru dalam teknologi informasi dan kejahatan siber (UU RI No 19, 2016). Proses penegakan hukum terhadap kejahatan dunia maya melibatkan penyelidikan dan forensik digital menggunakan alat dan teknik forensik untuk melacak dan menganalisis bukti digital. Dan kerjasama internasional dikarenakan kejahatan dunia maya sering melibatkan pelaku lintas negara, penegakan hukum sering melibatkan kerjasama internasional antara lembaga penegak hukum. Dalam implikasi hukum kejahatan dunia maya dapat mengakibatkan berbagai konsekuensi hukum, termasuk denda, hukuman penjara, dan tindakan hukum lainnya, tergantung pada jenis dan dampak kejahatan yang dilakukan. Keputusan hukum juga dapat mencakup kompensasi untuk korban dan perintah untuk mengembalikan atau menghentikan aktivitas ilegal (Kementerian Kominfo, 2020).

Dalam penelitian ini penulis menggunakan beberapa referensi penelitian terdahulu yang memiliki kaitan dengan pembahasan yang akan diteliti dalam jurnal ini. Adapun penelitian yang pertama dari Rafi Septia Budianto Pansariadi, dan Noenik Soekorini dengan jurnal yang berjudul "Tindak Pidana *Cyber Crime* dan PenegakanHukumnya" Penelitian tersebut membahas terkait permasalahan hukum normatif karena memberikan bobot yang sama antara metode konseptual dan perundang-undangan. Temuan studi ini menguatkan adanya pembatasan

kejahatan dunia maya di bawah hukum pidana positif Indonesia. Beberapa undang-undang lain, seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, dan KUHP sendiri mencerminkan pengaturan ini. Beberapa bentuk kejahatan dunia maya dapat dituntut berdasarkan hukum Indonesia, sementara yang lainnya tidak. Hal ini disebabkan fakta bahwa kejahatan dunia maya masih merupakan fenomena yang relatif muda. Sehubungan dengan itu, rancangan konsep KUHP yang baru telah dilaksanakan untuk melihat kebijakan hukum ke depan dalam memberantas dan menegakkan hukum yang berkaitan dengan kejahatan dunia maya. Selainitu, revisi Undang-Undang Informasi dan Transaksi Elektronik diperlukan untuk mengoptimalkan penegakan hukum terhadap *cyber crime* di Indonesia. Adapun penelitian yang kedua Arifah (2011) dengan jurnal yang berjudul "kasus *cyber crime* di Indonesia", dalam jurnal ini membahas tentang jenis-jenis kejahatan yang umum terjadi seperti penipuan daring dan pencurian data. Ia menyoroti lemahnya kesadaran masyarakat dan lemahnya sistem keamanan sebagai tantangan utama. Adapun Penelitian ketiga Banjarnahor (2013) dengan jurnal yang berjudul "Penerapan *cyberlaw* di Indonesia", dalam jurnal membahas dan menganalisis kendala dalam penegakan hukum terkait. Ia menekankan bahwa meskipun regulasi sudah ada melalui Undang-Undang ITE, masih terdapat kendala dalam penegakan hukumnya, terutama terkait literasi digital aparat penegak hukum dan kolaborasi internasional.

Penelitian-penelitian ini menggambarkan bagaimana hukum siber dan upaya pencegahan terus berkembang, meskipun masih banyak tantangan yang dihadapi. Beberapa tulisan atau penelitian yang telah disebutkan sebelumnya, menunjukan bahwa kajian atau penelitian terhadap permasalahan terkait yang ada di masyarakat tentang permasalahan *cyber crime* di Indonesia. Tetapi dari beberapa tulisan tersebut hanya mengkaji tentang perkembangan pembahasan apa yang disebut dengan *cyber crime*. Dalam penulisan jurnal ini, penulis mencoba menemukan pentingnya menjaga data-data pribadi terkana banyaknya kasus mengenai tindak pidana *cyber crime* yang ada di Indonesia saat ini. Mengingat hal ini, masuk akal bahwa hukum pidana dapat mencakup hal-hal seperti itu. Tidak mudah untuk membuat undang-undang pidana untuk memerangi kejahatan dunia maya mengingat sifat teknologi informasi yang terus berubah. Oleh karena itu, sangat penting bahwa penelitian di bidang ini dilakukan dari perspektif kebijakan hukum. Sekarang, sebagian besar sumber daya mereka dialokasikan untuk memerangi kejahatan online oleh organisasi penegakan hukum dan intelijen global, serta bisnis, pengecer, konsumen, dan pengguna akhir. Kejahatan dunia maya biasanya memulai dengan persetujuan host dan jaringan. Pelaku kejahatan, terutama yang menargetkan jaringan berbasis TCP/IP, umum di internet. Berdasarkan uraian di atas, penelitian ini berkonsentrasi pada peraturan hukum positif Indonesia tentang kejahatan dunia maya serta rencana hukum yang akan datang untuk menangani dan menerapkan hukum tersebut.

## METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan studi kasus. Data diperoleh dari literatur hukum yang ada serta kasus-kasus *cyber crime* yang telah terjadi di Indonesia. Analisis dilakukan terhadap peraturan perundang-undangan yang mengatur cyber crime di Indonesia serta efektivitas penegakan hukum yang berlaku.

## HASIL PENELITIAN DAN PEMBAHASAN

### Hukum Cyber Crime di Indonesia

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan landasan hukum utama untuk menindak pelaku *cyber crime* di Indonesia. Pasal-pasal dalam Undang-Undang Informasi dan Transaksi Elektronik menjelaskan perbuatan yang

dapat dikategorikan sebagai *cyber crime* dan sanksi yang dapat dikenakan. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengatur lebih lanjut tentang tanggung jawab penyelenggara sistem elektronik dalam melindungi data pengguna dan penanganan insiden keamanan siber. Hukum mengenai *cyber crime* (kejahatan dunia maya) di Indonesia mencakup berbagai regulasi dan undang-undang yang mengatur tindak kejahatan yang terjadi di ranah digital. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah landasan hukum utama yang mengatur kejahatan dunia maya di Indonesia. Undang-Undang ini mencakup berbagai aspek dari transaksi elektronik hingga kejahatan yang dilakukan melalui media elektronik.

Undang-Undang Informasi dan Transaksi Elektronik mengatur beberapa jenis kejahatan dunia maya, seperti, penipuan elektronik (Pasal 28 ayat (1) mengatur tentang tindakan penipuan melalui media elektronik, seperti phishing atau penipuan jual beli online. Pelanggaran data pribadi (Pasal 28 ayat (2) menetapkan larangan pengaksesan, penggunaan, atau penyebaran data pribadi secara ilegal. Penyebaran konten ilegal (Pasal 27 ayat (1) mengatur larangan penyebaran konten yang melanggar hukum, seperti pornografi atau ujaran kebencian. Undang-Undang Informasi dan Transaksi Elektronik memberikan sanksi pidana dan administratif bagi pelanggar, termasuk denda dan hukuman penjara. Misalnya, pelanggaran terhadap ketentuan Pasal 27 ayat (1) bisa dikenakan pidana penjara hingga 6 tahun dan/atau denda maksimum Rp1 miliar (UU ITE, 2008). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008. Undang-Undang Nomor 19 Tahun 2016 adalah amandemen dari Undang-Undang Informasi dan Transaksi Elektronik yang mengakomodasi perkembangan terbaru dalam teknologi informasi dan *cyber crime*. Perubahan ini memperjelas dan memperluas definisi serta sanksi terkait kejahatan dunia maya. Dengan adanya perubahan sangat penting seperti, penyebaran hoaks (Pasal 28 ayat (2), menambahkan ketentuan tentang penyebaran berita bohong atau hoaks yang dapat merugikan pihak tertentu atau masyarakat. Pencemaran nama baik (Pasal 27 ayat (3) menambah ketentuan mengenai pencemaran nama baik melalui media elektronik. Sanksi dalam perubahan ini memperkuat sanksi untuk kejahatan siber, seperti peningkatan masa hukuman penjara dan denda, serta memperluas cakupan tindakan yang dapat dikenakan hukuman (UU RI No 19, 2016).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur perlindungan data pribadi individu dalam ranah digital, termasuk hak individu untuk melindungi data pribadi mereka. Ketentuan tentang data pribadi, pengumpulan dan penggunaan data (Pasal 15 dan 16) mengatur bagaimana data pribadi dapat dikumpulkan dan digunakan, termasuk perlunya persetujuan dari individu. Hak akses dan koreksi (Pasal 23) memberikan hak kepada individu untuk mengakses dan mengoreksi data pribadi mereka yang dikelola oleh pihak lain.Sanksi Undang-Undang Perlindungan Data Pribadi menetapkan sanksi administratif, termasuk denda yang signifikan bagi pihak yang melanggar ketentuan perlindungan data pribadi (UU RI No 27, 2022). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, peraturan ini memberikan pedoman tentang penyelenggaraan sistem dan transaksi elektronik, termasuk aspek keamanan sistem informasi dan transaksi elektronik. Ketentuan tentang keamanan sistem elektronik (Pasal 6) mengatur kewajiban penyelenggara sistem elektronik untuk memastikan keamanan dan integritas sistem mereka. Pengelolaan Insiden Keamanan (Pasal 16) menetapkan prosedur untuk menangani dan melaporkan insiden keamanan siber. Peraturan ini mencakup sanksi administratif bagi penyelenggara sistem elektronik yang gagal mematuhi ketentuan keamanan (PP RI No 71, 2018).

Badan Siber dan Sandi Negara (BSSN) berfungsi sebagai lembaga yang mengawasi dan mengkoordinasikan keamanan siber di Indonesia. BSSN juga memberikan panduan dan

dukungan teknis dalam penanganan kejahatan dunia maya. Inisiatif dan kebijakan Badan Siber dan Sandi Negara (BSSN) menyusun dan menerapkan kebijakan nasional untuk melindungi infrastruktur siber. Badan Siber dan Sandi Negara (BSSN) menyediakan pelatihan dan edukasi mengenai keamanan siber kepada pemerintah dan sektor swasta (BSSN, 2021b). Kepolisian Republik Indonesia (Polri) memiliki unit khusus, yaitu Direktorat Tindak Pidana Siber, yang menangani penyelidikan dan penegakan hukum terhadap kejahatan dunia maya. Polri melakukan operasi untuk menangkap pelaku kejahatan siber dan mengamankan barang bukti. bekerja sama dengan lembaga internasional dalam menangani kejahatan siber lintas negara (Polisi Republik Indonesia, 2018). Dengan kerangka hukum ini, Indonesia berusaha untuk mengatasi dan menanggulangi kejahatan dunia maya yang terus berkembang dengan pesat.

**Kasus-Kasus Cyber Crime di Indonesia**

Kasus-kasus *cyber crime* di Indonesia mencerminkan berbagai bentuk kejahatan dunia maya yang terjadi dalam beberapa tahun terakhir. Pada tahun 2017, terjadi pembobolan data nasabah di salah satu bank besar di Indonesia. Pelaku menggunakan teknik phishing untuk mendapatkan informasi login dan data pribadi nasabah. Dengan informasi yang dicuri, pelaku melakukan transaksi yang tidak sah. Kasus ini mengakibatkan kerugian finansial yang signifikan bagi nasabah dan mengganggu reputasi bank tersebut. Penegakan hukum dan investigasi dilakukan oleh pihak kepolisian dan lembaga terkait untuk melacak pelaku (Kompas, 2017). Pada tahun 2020, sebuah sindikat internasional yang beroperasi di Indonesia terlibat dalam pencurian dan penyalahgunaan informasi kartu kredit. Sindikat ini mencuri data kartu kredit melalui teknik skimming dan phishing, kemudian menjual data tersebut di pasar gelap. Kasus ini melibatkan ribuan korban yang kehilangan uang dan mengalami kerusakan reputasi. Penegakan hukum melibatkan kerjasama internasional untuk menangkap pelaku dan mengamankan data yang dicuri (Detik, 2020). Pada tahun 2021, sebuah rumah sakit besar di Jakarta menjadi korban serangan ransomware. Data pasien dan sistem operasional rumah sakit terenkripsi oleh pelaku yang meminta tebusan untuk mengembalikan akses data. Serangan ini menyebabkan gangguan besar dalam layanan medis, termasuk penundaan prosedur dan perawatan pasien. Rumah sakit menghadapi kerugian finansial dan kerusakan pada data pasien (CNN Indonesia, 2021). Pada tahun 2018, terjadi kasus penyebaran hoaks melalui media sosial yang mengandung informasi palsu yang merugikan individu dan masyarakat. Beberapa akun media sosial menyebarkan berita bohong yang menyebabkan kerusuhan dan ketidakstabilan. Penyebaran hoaks ini menyebabkan kepanikan publik dan dampak sosial yang merugikan. Penegakan hukum dilakukan oleh pihak kepolisian dan kementerian terkait untuk menindak pelaku dan menghentikan penyebaran berita palsu (Tempo, 2018).

Adapun dua kasus besar terkait kejahatan dunia maya di Indonesia pencurian data nasabah bank oleh kelompok hacker internasional pada tahun 2020 dan serangan ransomware pada rumah sakit di Jakarta pada tahun 2022. Kasus Pencurian Data Nasabah Bank oleh Kelompok Hacker Internasional (2020), kelompok hacker internasional berhasil membobol data nasabah dari beberapa bank di Indonesia. Kelompok ini menggunakan teknik phishing dan malware untuk mengakses informasi pribadi dan keuangan nasabah. Mereka mencuri data login dan informasi kartu kredit, yang kemudian digunakan untuk melakukan transaksi ilegal dan penipuan. Proses penegakan hukum Kepolisian Indonesia, khususnya Direktorat Tindak Pidana Siber (*Dittipidsiber*), melakukan investigasi menyeluruh terhadap kasus ini. Penegakan hukum melibatkan penyelidikan digital menggunakan forensik digital untuk melacak jejak digital pelaku dan menganalisis metode serangan yang digunakan. Kerjasama Internasional dan berkoordinasi dengan lembaga penegak hukum internasional dan perusahaan teknologi untuk melacak dan menangkap pelaku. Tindakan Preventif dengan meningkatkan keamanan sistem

perbankan dan melakukan sosialisasi kepada nasabah mengenai risiko phishing dan penipuan online. Kasus ini menyebabkan kerugian finansial yang signifikan bagi nasabah dan bank yang terkena dampak. Selain itu, reputasi bank juga terpengaruh akibat serangan tersebut. Penegakan hukum berhasil mengidentifikasi beberapa pelaku dan memulihkan sebagian data yang dicuri (Kompas, 2020).

Kasus Ransomware di Rumah Sakit Jakarta Pada tahun 2022, sebuah rumah sakit besar di Jakarta menjadi korban serangan ransomware. Serangan ini mengakibatkan enkripsi data pasien dan sistem operasional rumah sakit. Para pelaku ransomware meminta tebusan dalam bentuk *cryptocurrency* untuk mendekripsi data dan mengembalikan akses. Proses penegakan hukum Kepolisian Republik Indonesia melalui Direktorat Tindak Pidana Siber melakukan penyelidikan untuk mengidentifikasi pelaku dan menganalisis metode serangan. Rumah sakit bekerja sama dengan ahli keamanan siber untuk menangani dan memulihkan data yang terenkripsi serta memperkuat sistem keamanan untuk mencegah serangan serupa di masa depan. Karena serangan ransomware sering melibatkan pelaku lintas negara, kepolisian melakukan koordinasi dengan lembaga internasional dalam penanganan kasus ini. Serangan ransomware ini menyebabkan gangguan besar dalam pelayanan kesehatan, termasuk penundaan dalam prosedur medis dan perawatan pasien. Kerusakan data juga mempengaruhi operasi rumah sakit dan menimbulkan biaya tambahan untuk pemulihan sistem dan data (CNN Indonesia, 2021). Kedua kasus ini menunjukkan dampak serius dari kejahatan dunia maya terhadap sektor perbankan dan layanan kesehatan di Indonesia. Penegakan hukum dan tindakan preventif yang efektif sangat penting untuk melindungi data dan sistem dari ancaman *cyber*. Kasus-kasus ini menggambarkan bagaimana kejahatan dunia maya di Indonesia dapat mempengaruhi berbagai sektor dan mengakibatkan kerugian yang signifikan. Penegakan hukum dan langkah-langkah pencegahan yang efektif sangat penting untuk mengatasi dan mengurangi dampak dari kejahatan siber.

Para ahli hukum di Indonesia memberikan berbagai tanggapan mengenai kasus *cyber crime*, terutama terkait regulasi dan tantangan penegakan hukumnya. Ahli hukum Arief Hidayat, misalnya, menekankan bahwa Undang-Undang Informasi dan Transaksi Elektronik memang menjadi landasan utama penanganan *cyber crime* di Indonesia, namun beberapa pasal di dalamnya memerlukan revisi agar lebih efektif. Ia menyoroti bahwa pasal-pasal mengenai pencemaran nama baik dan penghinaan sering kali menimbulkan kontroversi, dan perlu ada batasan yang lebih jelas untuk melindungi kebebasan berpendapat tanpa mengabaikan keadilan. Menurut Banjarnahor (2013), kendala terbesar dalam penegakan hukum *cyber crime* adalah literasi digital penegak hukum dan kurangnya fasilitas teknologi forensik. Banyak kasus *cyber crime* sulit ditangani karena kurangnya alat dan keterampilan yang memadai untuk melacak bukti digital. Ia juga menyoroti pentingnya kerja sama internasional mengingat banyak kasus melibatkan pelaku lintas negara. Ahli hukum seperti Melani, Disemadi, & Jaya (2020) berpendapat bahwa perlindungan korban *cyber crime*, terutama yang berkaitan dengan kejahatan ekonomi dan privasi, masih kurang diperhatikan. Mereka mengusulkan adanya kebijakan yang lebih kuat untuk melindungi korban dari dampak kejahatan siber, baik dari segi keuangan maupun data pribadi. Daud (2013) menekankan pentingnya kerja sama internasional dalam penanganan *cyber crime*, karena kejahatan ini sering kali melibatkan pelaku lintas batas. Indonesia perlu memperkuat kolaborasi dengan negara lain serta lembaga seperti Interpol untuk menangani kasus *cyber crime* secara efektif. Secara keseluruhan, para ahli sepakat bahwa meskipun Indonesia memiliki regulasi yang cukup kuat melalui Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi, penegakannya masih memerlukan penguatan, terutama dalam literasi digital aparat hukum, perlindungan korban, dan kerja sama internasional.

**Upaya Pencegahan dan Penanganan**

Upaya pencegahan dan penanganan kejahatan dunia maya di Indonesia melibatkan berbagai strategi dan tindakan yang melibatkan pemerintah, sektor swasta, lembaga penegak hukum, dan masyarakat. Upaya pencegahan melalui regulasi dan kebijakan, Undang-Undang dan Peraturan Undang-Undang ITE (Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik) menetapkan kerangka hukum untuk mengatur aktivitas di dunia maya, termasuk pencegahan kejahatan siber. Amendemen Undang-Undang Informasi dan Transaksi Elektronik pada tahun 2016 memperbarui ketentuan untuk menangani perkembangan teknologi. Undang-Undang Perlindungan Data Pribadi (Undang-Undang Nomor 27 Tahun 2022) mengatur perlindungan data pribadi dan privasi individu, serta menetapkan sanksi bagi pelanggaran. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menetapkan pedoman untuk keamanan sistem elektronik dan penanganan insiden keamanan.

Pendidikan dan Kesadaran seperti pelatihan keamanan siber, Badan Siber dan Sandi Negara (BSSN) menyediakan pelatihan dan edukasi tentang keamanan siber kepada pemerintah, sektor swasta, dan masyarakat umum untuk meningkatkan kesadaran dan kesiapan menghadapi ancaman siber. Kampanye kesadaran Anti-Phishing dan keamanan data melakukan kampanye informasi untuk meningkatkan kesadaran tentang teknik phishing, penggunaan password yang kuat, dan praktik keamanan online lainnya. Adapun penguatan infrastruktur keamanan jaringan dan sistem dengan cara penerapan teknologi keamanan menggunakan perangkat lunak keamanan, firewall, dan sistem deteksi intrusi untuk melindungi jaringan dan sistem dari serangan. Standarisasi keamanan dengan standar Internasional mengadopsi standar internasional untuk keamanan informasi, seperti ISO/IEC 27001, untuk memastikan bahwa sistem dan data terlindungi dengan baik. Upaya penanganan penegakan hukum dengan cara investigasi dan penindakan Direktorat Tindak Pidana Siber (Dittipidsiber) Polri menangani kasus kejahatan siber dengan menggunakan forensik digital, investigasi, dan penangkapan pelaku. Direktorat ini juga melakukan operasi *cyber crime* untuk menangkap sindikat kejahatan siber. Kerjasama Interpol dan Europol berkolaborasi dengan lembaga internasional untuk menangani kejahatan siber lintas negara. Kerjasama ini melibatkan pertukaran informasi dan koordinasi operasional.

Tanggapan dan pemulihan Tim Respon Insiden Keamanan (CSIRT), tim yang dibentuk untuk merespons insiden keamanan siber, menangani dan memitigasi dampak dari serangan, serta melakukan pemulihan sistem. Pemulihan Data dengan cara *Backups* dan *Recovery* melakukan backup data secara teratur dan mengembangkan rencana pemulihan bencana untuk memastikan bahwa data dapat dipulihkan jika terjadi serangan atau kerusakan. Dukungan dan bantuan layanan konsultasi BSSN dan Penyedia Layanan Keamanan menyediakan layanan konsultasi dan bantuan teknis bagi organisasi dan individu yang menghadapi masalah keamanan siber. Dengan adanya *Platform* pelaporan menyediakan saluran bagi masyarakat untuk melaporkan insiden kejahatan siber, seperti portal aduan untuk penipuan online dan phishing. Contoh Implementasi Upaya Pencegahan dan Penanganan dengan kampanye "Bersama Kita Cegah *Cyber Crime*" Kampanye yang diluncurkan oleh BSSN untuk meningkatkan kesadaran tentang ancaman cyber dan praktik keamanan (BSSN, 2021). Operasi *cyber crime* Polri operasi yang dilakukan oleh Polri untuk menangkap pelaku kejahatan siber dan mengamankan barang bukti (Polri, 2021). Program Pendidikan Keamanan Siber oleh BSSN program pelatihan dan edukasi untuk meningkatkan kesadaran keamanan siber di kalangan pelajar, profesional, dan masyarakat (BSSN, 2021).

Upaya pencegahan dan penanganan kejahatan dunia maya merupakan usaha berkelanjutan yang memerlukan kerjasama antara berbagai pihak untuk melindungi data dan

sistem dari ancaman yang terus berkembang. Dalam menghadapi ancaman kejahatan siber lintas negara, pemerintah Indonesia telah meningkatkan kerjasama dengan institusi internasional dan melakukan penguatan kapasitas lembaga penegak hukum, khususnya dalam bidang forensik digital. Kerjasama internasional dalam menangani kejahatan siber lintas negara, Interpol menyediakan platform untuk pertukaran informasi dan koordinasi internasional dalam penanganan kejahatan siber. Negara anggota, termasuk Indonesia, dapat berbagi intelijen dan strategi dalam menghadapi sindikat kejahatan siber yang beroperasi lintas batas (Interpol, 2021). Europol mendukung kerjasama antara negara-negara anggota Uni Eropa dan mitra internasional, termasuk Indonesia, dalam hal penegakan hukum terhadap kejahatan siber. Europol menawarkan dukungan teknis dan strategis dalam penyelidikan kasus kejahatan siber besar (Europol, 2021). *United Nations Office on Drugs and Crime* (UNODC) memberikan dukungan teknis dan pelatihan untuk meningkatkan kapasitas negara-negara dalam menangani kejahatan siber. Ini termasuk pembuatan dan pelaksanaan kebijakan serta strategi untuk memerangi kejahatan siber (UNODC, 2021). Kepolisian Internasional (Interpol) dan Kerjasama Regional melalui kerjasama regional seperti ASEAN, Indonesia berkolaborasi dengan negara-negara tetangga untuk menangani kejahatan siber yang mempengaruhi kawasan tersebut (ASEAN, 2021). Penguatan Kapasitas Lembaga Penegak Hukum dalam Forensik Digital lembaga penegak hukum di Indonesia, seperti Direktorat Tindak Pidana Siber (Dittipidsiber) Polri, secara rutin mengikuti pelatihan dan sertifikasi internasional dalam forensik digital. Pelatihan ini mencakup teknik-teknik terbaru dalam analisis digital dan investigasi kejahatan siber (BSSN, 2021).

Pengadaan Peralatan dan Teknologi investasi dalam perangkat keras dan perangkat lunak forensik digital yang canggih untuk mendukung investigasi. Peralatan ini digunakan untuk menganalisis dan memulihkan data yang hilang atau terenkripsi selama serangan siber (Polri, 2021). Kerjasama dengan akademisi dan industri dengan cara kolaborasi antara lembaga penegak hukum dengan universitas dan perusahaan teknologi untuk penelitian dan pengembangan teknik forensik digital baru (UI, 2020). Peningkatan Kesadaran Masyarakat tentang Keamanan Informasi dan Penggunaan Perangkat Lunak Keamanan Pemerintah dan organisasi keamanan siber meluncurkan kampanye untuk meningkatkan kesadaran tentang pentingnya menjaga informasi pribadi dan praktik keamanan siber yang baik. Kampanye ini mencakup penggunaan media sosial, seminar, dan workshop (BSSN, 2021). Edukasi di sekolah dan komunitas dalam program pendidikan yang menyasar siswa dan masyarakat umum mengenai keamanan siber dan penggunaan perangkat lunak keamanan. Ini termasuk kurikulum yang mengajarkan praktik terbaik dalam menggunakan internet dan perangkat digital (Kementerian Kominfo, 2020). Penggunaan Perangkat Lunak Keamanan Pemerintah dan lembaga keamanan siber merekomendasikan penggunaan perangkat lunak keamanan yang terpercaya, seperti antivirus dan firewall, untuk melindungi perangkat dari ancaman siber (BSSN, 2020). Update dan pemeliharaan sistem masyarakat disarankan untuk secara rutin memperbarui sistem operasi dan aplikasi mereka untuk memastikan perlindungan dari kerentanan terbaru dan ancaman siber (Kominfo, 2021). Pencegahan dan penanganan kejahatan siber memerlukan pendekatan multifaset yang melibatkan kerjasama internasional, penguatan kapasitas penegak hukum, serta peningkatan kesadaran dan pendidikan masyarakat. Dengan upaya-upaya ini, Indonesia dapat lebih efektif dalam menghadapi tantangan kejahatan siber dan melindungi data serta sistem dari ancaman yang terus berkembang.

## KESIMPULAN

Berdasarkan penelitian yang dilakukan, Indonesia telah memiliki kerangka hukum yang cukup kuat untuk menangani tindak pidana cyber crime melalui Undang-Undang Nomor 11

Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan amandemennya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Peraturan-peraturan ini menjadi landasan bagi upaya pencegahan dan penindakan terhadap kejahatan siber, terutama di sektor keuangan, kesehatan, dan telekomunikasi. Meskipun demikian, tantangan utama yang dihadapi Indonesia dalam penegakan hukum siber adalah kemampuan penegak hukum dalam menerapkan teknologi forensik digital, rendahnya literasi digital masyarakat, dan kerjasama internasional yang masih belum optimal. Tantangan ini membuat upaya penanggulangan *cyber crime* menjadi kompleks, terutama karena sifat kejahatan siber yang lintas batas dan terus berkembang seiring inovasi teknologi. Oleh karena itu, diperlukan peningkatan kapasitas dan kompetensi penegak hukum dalam memanfaatkan teknologi canggih, penguatan kebijakan perlindungan data yang lebih ketat, serta peningkatan kesadaran masyarakat mengenai pentingnya keamanan siber. Selain itu, kerjasama internasional dalam menangani kejahatan lintas negara menjadi sangat penting untuk meningkatkan efektivitas penegakan hukum di bidang ini.Dengan pendekatan multifaset ini, Indonesia diharapkan dapat lebih siap dalam menghadapi tantangan cyber crime yang terus berkembang dan menjaga integritas data serta keamanan digital masyarakat.

**DAFTAR PUSTAKA**

Asean. (2021). Cybercrime Cooperation. Https://Asean.Org/Asean-Economic-Community/Sectoral-Bodies-Other/Finance-And-Economics/Cybercrime/

Bank Indonesia. (2009). Penguatan Pengaturan Dan Pengawasan Perbankan Dalam Menghadapi Kejahatan Dunia Maya. Jakarta: Bank Indonesia.

Bsa. (2010). The Software Alliance "2010 Global Software Piracy Study. Https://Global.Bsa.Org/.

Bssn. (2020). Rekomendasi Perangkat Lunak Keamanan. Badan Siber Dan Sandi Negara. Https://Www.Bssn.Go.Id/Rekomendasi-Perangkat-Lunak-Keamanan/

Bssn. (2021a). Kampanye Cyber Crime. Badan Siber Dan Sandi Negara. Https://Www.Bssn.Go.Id/Kampanye-Cyber-Crime/

Bssn. (2021b). Laporan Keamanan Siber Di Indonesia: Ancaman Dan Respons. Badan Siber Dan Sandi Negara.

Bssn. (2021c). Program Pendidikan Keamanan Siber. Badan Siber Dan Sandi Negara. Https://Www.Bssn.Go.Id/Program-Pendidikan-Keamanan-Siber/

Cnn Indonesia. (2021). Rumah Sakit Jakarta Kena Serangan Ransomware. Https://Www.Cnnindonesia.Com/Teknologi/20211014105422-185-702029/Rumah-Sakit-Jakarta-Kena-Serangan-Ransomware.

Detik. (2020). Sindikat Penipuan Kartu Kredit Terbesar Ditangkap. Https://News.Detik.Com/Berita/D-5189875/Sindikat-Penipuan-Kartu-Kredit-Terbesar-Ditangkap.

Europol. (2021). Cybercrime. Https://Www.Europol.Europa.Eu/Activities-Services/Services-Support/Cybercrime

Fadhli, Z., & Bahri, S. (2020). Perlindungan Hukum Terhadap Pelanggan Jasa Telekomunikasi Dalam Registrasi Kartu Seluler Prabayar Melalui Gerai (Suatu Penelitian Di Kota Banda Aceh). Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan 4, 2, 743–751.

Garnett, H. A., & James, T. S. (2020). Cyber Elections In The Digital Age: Threats And Opportunities Of Technology For Electoral Integrity. Election Law Journal: Rules, Politics, And Policy 19, 2, 111–126.

Interpol. (2021). Cybercrime. Https://Www.Interpol.Int/En/Crimes/

Kementerian Kominfo. (2020). Kementerian Komunikasi Dan Informatika Republik Indonesia. (2020). "Strategi Nasional Keamanan Siber 2020.

Kominfo. (2021). Pentingnya Update Sistem. Https://Www.Kominfo.Go.Id/Content/Detail/32800/Pentingnya-Update-Sistem-Dan-Aplikasi/0/Berita

Kompas. (2017). Pembobolan Data Bank Di Indonesia. Https://Nasional.Kompas.Com/Read/2017/10/24/13301771/Pembobolan-Data-Nasabah-Bank-Dan-Cara-Kerja-Penjahat-Siber.

Kompas. (2020). Hacker Internasional Bobol Data Nasabah Bank Di Indonesia. Https://Nasional.Kompas.Com/Read/2020/11/19/14021531/Hacker-Internasional-Bobol-Data-Nasabah-Bank-Di-Indonesia

Koos, S. (2022). Digital Globalization And Law. Lex Scientia Law Review 6, 1, 33–68.

Lubis, M. A. (2020). Penegakan Hukum Terhadap Cybercrime Dalam Perspektif Hukum Pidana Nasional. Jurnal Penegakan Hukum Dan Keadilan, 5(1), 102–119.

Ojk. (2019). Laporan Pengawasan Dan Keamanan Siber Di Sektor Keuangan. Jakarta: Ojk.

Ojk. (2020). Laporan Tahunan Keamanan Siber Di Sektor Perbankan. Jakarta: Ojk.

Polisi Republik Indonesia. (2018). Laporan Penangkapan Sindikat Penyebaran Konten Pornografi Di Indonesia. Jakarta: Divisi Humas Polri.

Polri. (2021). Operasi Cybercrime. Https://Www.Polri.Go.Id/Operasi-Cybercrime

Pp Ri No 71. (2018). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. Https://Peraturan.Bpk.Go.Id/Home/Details/124639/Pp-No-71-Tahun-2019.

Putro, W. D. (2019). Pancasila Di Era Paska Ideologi. Veritas Et Justitia 5, 1, 1–19.

Shidarta. (2022). Multisentrisme Humaniora Digital: Filsafat Hukum Masa Depan Dan Masa Depan Filsafat Hukum. Binus University, Jakarta.

Soekanto, S. (2019). Tinjauan Hukum Cybercrime Di Indonesia Dalam Era Digitalisasi. Jurnal Hukum Dan Pembangunan, 39(2), 301–316.

Tempo. (2018). Kasus Penyebaran Hoaks Yang Mengguncang Masyarakat. Https://Nasional.Tempo.Co/Read/1090846/Kasus-Penyebaran-Hoaks-Yang-Mengguncang-Masyarakat

Ui. (2020). Penelitian Forensik Digital. Universitas Indonesia. Https://Www.Ui.Ac.Id/Penelitian-Forensik-Digital

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Unodc. (2021). Cybercrime. United Nations Office On Drugs And Crime. Https://Www.Unodc.Org/Unodc/En/Cybercrime/

Widhiyanti, H. N. (2020). The Urgency Of Harmonizing Competition Laws In Moving Towards The Asean Free Trade Area,Fiat Justisia. Jurnal Ilmu Hukum 14, 1, 45–68.