PENEGAKAN HUKUM TINDAK PIDANA *CYBER CRIME* DITINJAU DARI UNDANG-UNDANG NOMOR 1 TAHUN 2024 TENTANG INFORMASI TRANSAKSI ELEKTRONIK [1]

Oleh :
Amelia Anna Mangundap [2]
Nurhikmah Nachrawy [3]
Anna S. Wahongan [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui dan memahami pengaturan hukum terhadap tindak pidana *cyber crime* dan untuk mengetahui dan memahami penegakan hukum tindak pidana cyber crime ditinjau dari undang-undang nomor 1 tahun 2024 tentang informasi transaksi elektronik. Dengan menggunakan metode penelitian yuridis normatif, dapat ditarik kesimpulan yaitu : 1. Berdasarkan pembahasan mengenai faktor penyebab terjadinya cyber crime, dapat disimpulkan bahwa kejahatan siber merupakan fenomena yang kompleks dan dipengaruhi oleh berbagai faktor yang saling berkaitan. Faktor utama yang mendorong terjadinya cyber crime meliputi perkembangan teknologi yang pesat tanpa diimbangi dengan sistem keamanan yang memadai, faktor ekonomi yang memotivasi pelaku untuk memperoleh keuntungan secara instan, serta rendahnya kesadaran hukum dan literasi digital masyarakat. Selain itu, faktor sosial dan psikologis seperti anonimitas di dunia maya dan dorongan untuk menguji kemampuan juga turut berkontribusi terhadap meningkatnya kejahatan siber. 2. Dalam hal penanggulangan tindak pidana cyber crime ditinjau dari Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, dapat disimpulkan bahwa regulasi tersebut telah memberikan dasar hukum yang cukup komprehensif dalam menangani kejahatan siber di Indonesia. Undang-undang ini mengatur berbagai bentuk perbuatan yang dilarang serta memberikan sanksi pidana yang tegas bagi pelaku cyber crime.

Kata Kunci : *cyber crime, UU ITE*

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam seluruh aspek kehidupan manusia, termasuk dalam bidang sosial, ekonomi, dan hukum. Di satu sisi, kemajuan teknologi digital memberikan kemudahan dalam bertransaksi dan berkomunikasi secara cepat dan efisien, namun di sisi lain, kemajuan ini juga melahirkan berbagai bentuk kejahatan baru yang dikenal dengan istilah *cyber crime* atau kejahatan siber. *Cyber crime* merupakan bentuk tindak pidana yang dilakukan melalui jaringan internet dengan memanfaatkan teknologi informasi untuk tujuan melawan hukum seperti penipuan online, akses ilegal, penyebaran konten terlarang, serta perjudian daring.[5]

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 yang dianggap sudah tidak relevan sepenuhnya dengan perkembangan teknologi dan dinamika sosial masyarakat. Perubahan ini mencakup penyesuaian terhadap beberapa pasal, antara lain mengenai delik penghinaan dan pencemaran nama baik, penyebaran informasi bohong, serta penguatan aspek perlindungan data pribadi.[6]

Dalam praktiknya, penerapan hukum terhadap pelaku *cyber crime* masih menghadapi banyak tantangan, baik dari sisi penegakan hukum, kapasitas aparat, maupun dari sisi regulasi yang masih perlu harmonisasi dengan peraturan internasional. Tantangan ini membuat kebijakan hukum nasional perlu terus diperbarui agar mampu menghadapi bentuk-bentuk kejahatan baru di dunia digital.[7]

Seperti contoh kasus yakni Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr, perkara ini berkaitan dengan tindak pidana *cyber crime* berupa akses ilegal terhadap sistem elektronik yang dilakukan oleh terdakwa dengan cara meretas sistem digital untuk memperoleh dokumen elektronik tanpa hak. Dalam putusan tersebut, terdakwa terbukti secara sah dan meyakinkan melanggar ketentuan Pasal 30 ayat (2) juncto Pasal 46 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 220711010392
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Doktor Ilmu Hukum

[5] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Prenadamedia Group, Jakarta, 2018, hlm. 67.
[6] Kementerian Komunikasi dan Informatika RI, *Naskah Akademik Perubahan UU ITE*, Jakarta, 2023, hlm. 9.
[7] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, RajaGrafindo Persada, Jakarta, 2018, hlm. 89.

FAKULTAS HUKUM UNSRAT 2026

ITE). Terdakwa diketahui melakukan akses terhadap sistem elektronik tertentu dengan menggunakan sarana komputer dan akun digital untuk memperoleh data elektronik yang bersifat terbatas. Perbuatan tersebut dipandang sebagai tindakan melawan hukum karena dilakukan tanpa izin dari pemilik sistem elektronik yang sah. Majelis hakim dalam pertimbangannya menilai bahwa unsur "dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik" telah terpenuhi berdasarkan alat bukti elektronik, keterangan saksi, serta barang bukti digital yang diajukan di persidangan.

Kasus tersebut menunjukkan bahwa perkembangan teknologi informasi telah memunculkan berbagai bentuk kejahatan siber yang dapat mengancam keamanan data dan sistem elektronik di Indonesia. Tindak pidana peretasan tidak hanya merugikan pihak tertentu secara materiil, tetapi juga berpotensi mengganggu keamanan informasi dan perlindungan data pribadi masyarakat. Dalam perkara ini, pengadilan menegaskan bahwa penggunaan teknologi digital secara melawan hukum dapat dikenakan pertanggungjawaban pidana berdasarkan ketentuan UU ITE sebagai instrumen hukum siber di Indonesia. Putusan tersebut juga mencerminkan komitmen aparat penegak hukum dalam menanggulangi kejahatan digital melalui penerapan alat bukti elektronik dan pemeriksaan digital forensik dalam proses pembuktian. Oleh karena itu, perkara ini menjadi contoh konkret penerapan hukum pidana siber terhadap pelaku akses ilegal sistem elektronik serta pentingnya perlindungan hukum terhadap keamanan ruang digital di Indonesia.

Penelitian ini menjadi penting karena memberikan kontribusi ilmiah dalam memahami bagaimana kebijakan hukum nasional, khususnya setelah berlakunya Undang-Undang Nomor 1 Tahun 2024 tentang ITE, berperan dalam menanggulangi kejahatan siber di Indonesia. Selain itu, penelitian ini diharapkan dapat memberikan rekomendasi bagi pembuat kebijakan agar penegakan hukum di bidang siber menjadi lebih efektif dan berkeadilan.[8]

B. Rumusan Masalah

1. Bagaimana pengaturan hukum terhadap tindak pidana *cyber crime*?
2. Bagaimana penegakan hukum tindak pidana cyber crime ditinjau dari undang-undang nomor 1 tahun 2024 tentang informasi transaksi elektronik?

C. Metode Penelitian

Metode pendekatan yang digunakan dalam penelitian ini adalah Metode Yuridis Normatif.

PEMBAHASAN

A. Pengaturan Hukum Terhadap Tindak Pidana Cyber Crime

Pengaturan hukum terhadap tindak pidana cyber crime di Indonesia pada awalnya masih menggunakan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP). Akan tetapi, perkembangan teknologi informasi yang sangat cepat menyebabkan banyak bentuk kejahatan siber tidak dapat dijangkau secara optimal oleh ketentuan pidana konvensional. Oleh karena itu, negara membentuk regulasi khusus melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian mengalami beberapa perubahan hingga Undang-Undang Nomor 1 Tahun 2024. Pembentukan regulasi tersebut bertujuan menyesuaikan hukum pidana dengan perkembangan teknologi digital modern.[9]

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik menjadi dasar hukum utama dalam pengaturan tindak pidana cyber crime di Indonesia. Undang-undang tersebut mengatur berbagai bentuk perbuatan yang dikategorikan sebagai tindak pidana siber, seperti akses ilegal terhadap sistem elektronik, manipulasi data elektronik, penyebaran informasi elektronik yang melanggar hukum, dan intersepsi ilegal. Pengaturan tersebut menunjukkan bahwa negara berupaya memberikan perlindungan terhadap keamanan sistem elektronik dan data digital masyarakat. Dengan demikian, hukum tidak hanya berfungsi sebagai alat pengendalian sosial, tetapi juga sebagai sarana perlindungan ruang digital nasional.

Dalam Pasal 30 Undang-Undang ITE diatur bahwa setiap orang dilarang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain. Ketentuan ini menjadi dasar hukum terhadap tindakan peretasan (*hacking*) yang merupakan salah satu bentuk cyber crime paling umum terjadi. Selain itu, Pasal 32 Undang-Undang ITE juga melarang setiap orang memindahkan, mengubah, menghilangkan, atau menyembunyikan informasi elektronik milik

[8] Marwan Effendy, *Perkembangan Hukum Pidana dan Kriminologi*, PT Refika Aditama, Bandung, 2020, hlm. 64.

[9] Soerjono Soekanto, *Pokok-Pokok Sosiologi Hukum*, Jakarta: Raja Grafindo Persada, 2006, hlm. 20.

FAKULTAS HUKUM UNSRAT 2026

pihak lain tanpa hak. Ketentuan tersebut menunjukkan bahwa perlindungan hukum tidak hanya diberikan terhadap sistem elektronik, tetapi juga terhadap data dan dokumen elektronik.

Selain mengatur larangan, Undang-Undang ITE juga mengatur sanksi pidana terhadap pelaku cyber crime. Dalam Pasal 46 Undang-Undang ITE ditegaskan bahwa setiap orang yang melanggar ketentuan Pasal 30 dapat dipidana dengan pidana penjara dan/atau denda. Pengaturan sanksi pidana tersebut bertujuan memberikan efek jera kepada pelaku dan mencegah terjadinya kejahatan siber yang dapat merugikan masyarakat. Oleh sebab itu, keberadaan sanksi pidana menjadi bagian penting dalam penegakan hukum terhadap cyber crime di Indonesia.[10]

Pengaturan hukum terhadap cyber crime juga berkaitan dengan pengakuan alat bukti elektronik dalam sistem hukum Indonesia. Pasal 5 Undang-Undang ITE menyatakan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang sah. Ketentuan tersebut menjadi sangat penting karena tindak pidana cyber crime umumnya meninggalkan jejak digital yang hanya dapat dibuktikan melalui alat bukti elektronik. Dengan demikian, hukum acara pidana di Indonesia mengalami perkembangan dengan mengakui alat bukti elektronik sebagai bagian dari proses pembuktian di pengadilan.

Seperti contoh kasus yakni Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr yang berkaitan dengan akses ilegal terhadap sistem elektronik pemerintah daerah. Dalam perkara tersebut, terdakwa terbukti melakukan akses tanpa hak terhadap situs *sitepak.bekasikab.go.id* untuk memperoleh dokumen elektronik tertentu. Tindakan tersebut dilakukan dengan menggunakan perangkat elektronik dan akun tertentu tanpa izin resmi dari pihak yang berwenang. Kasus ini menunjukkan bahwa sistem elektronik pemerintah dapat menjadi sasaran tindak pidana siber apabila tidak memiliki perlindungan keamanan yang memadai.

Dalam pertimbangan hukumnya, majelis hakim menilai bahwa terdakwa telah memenuhi unsur tindak pidana sebagaimana diatur dalam Pasal 30 ayat (2) jo. Pasal 46 ayat (2) Undang-Undang ITE. Hakim menyatakan bahwa tindakan mengakses sistem elektronik milik orang lain tanpa hak merupakan bentuk perbuatan melawan hukum yang dapat dipidana. Pertimbangan tersebut menunjukkan bahwa pengaturan hukum terhadap cyber crime telah memiliki dasar normatif yang jelas dalam hukum positif Indonesia. Dengan demikian, penegakan hukum terhadap tindak pidana siber dapat dilakukan secara efektif melalui ketentuan dalam Undang-Undang ITE.

Kasus Putusan Pengadilan Negeri Cikarang tersebut juga menunjukkan pentingnya perlindungan terhadap sistem elektronik milik pemerintah. Sistem elektronik pemerintah mengandung berbagai data dan dokumen penting yang berkaitan dengan pelayanan publik dan administrasi negara. Oleh sebab itu, akses ilegal terhadap sistem tersebut dapat mengganggu keamanan informasi publik dan menimbulkan kerugian bagi negara maupun masyarakat. Pengaturan hukum cyber crime menjadi instrumen penting dalam menjaga stabilitas dan keamanan sistem elektronik nasional.[11]

Dalam perspektif hukum pidana, cyber crime termasuk kategori tindak pidana khusus karena memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Cyber crime dilakukan melalui media elektronik sehingga memerlukan pendekatan penegakan hukum yang lebih modern dan berbasis teknologi. Pembuktian tindak pidana siber membutuhkan kemampuan digital forensik dan alat bukti elektronik yang memadai. Oleh sebab itu, pengaturan hukum cyber crime tidak dapat dipisahkan dari perkembangan teknologi informasi dan sistem keamanan digital.[12]

Dalam praktiknya, cyber crime sering menimbulkan kerugian besar baik secara materiil maupun immateriil. Kerugian tersebut dapat berupa pencurian data pribadi, kerugian finansial, pencemaran nama baik digital, hingga gangguan terhadap sistem elektronik negara. Oleh sebab itu, pengaturan hukum cyber crime tidak hanya bertujuan menghukum pelaku, tetapi juga melindungi masyarakat dari dampak negatif perkembangan teknologi informasi. Hal ini menunjukkan bahwa hukum memiliki fungsi preventif dan represif dalam penanggulangan tindak pidana siber.

Pengaturan hukum terhadap cyber crime juga harus didukung dengan peningkatan kapasitas aparat penegak hukum di bidang teknologi informasi. Aparat penegak hukum perlu memahami mekanisme kerja sistem elektronik dan metode digital forensik agar mampu mengungkap tindak pidana siber secara efektif.

[10] Undang-Undang Informasi dan Transaksi Elektronik, Pasal 46.

[11] Edmon Makarim, *Pengantar Hukum Telematika*, Jakarta: Raja Grafindo Persada, 2005, hlm. 160.

[12] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2008, hlm. 70.

FAKULTAS HUKUM UNSRAT 2026

Selain itu, masyarakat juga perlu diberikan edukasi mengenai keamanan digital agar tidak mudah menjadi korban cyber crime. Dengan demikian, penanggulangan cyber crime memerlukan sinergi antara regulasi hukum, teknologi keamanan, dan kesadaran hukum masyarakat.[13]

Dalam perspektif sosiologi hukum, pengaturan cyber crime menunjukkan bahwa hukum selalu berkembang mengikuti perubahan sosial dan teknologi masyarakat. Perkembangan ruang digital menyebabkan hukum harus mampu menyesuaikan diri dengan bentuk-bentuk kejahatan baru yang sebelumnya tidak dikenal dalam hukum pidana konvensional. Oleh sebab itu, pembentukan Undang-Undang ITE merupakan bentuk respons negara terhadap dinamika perkembangan teknologi informasi di era digital.

Pengaturan hukum terhadap cyber crime pada akhirnya bertujuan menciptakan keamanan, ketertiban, dan kepastian hukum dalam penggunaan teknologi informasi. Negara melalui Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik berupaya memberikan perlindungan terhadap sistem elektronik dan kepentingan masyarakat di ruang digital. Dengan adanya pengaturan tersebut, masyarakat diharapkan dapat menggunakan teknologi informasi secara aman, bertanggung jawab, dan sesuai dengan ketentuan hukum yang berlaku.[14]

Perkembangan teknologi digital yang sangat pesat telah menyebabkan ruang siber menjadi bagian penting dalam kehidupan masyarakat modern. Aktivitas ekonomi, pendidikan, pemerintahan, hingga komunikasi sosial saat ini banyak dilakukan melalui sistem elektronik dan jaringan internet. Namun demikian, perkembangan tersebut juga meningkatkan potensi terjadinya tindak pidana siber yang dapat merugikan masyarakat maupun negara. Oleh sebab itu, pengaturan hukum terhadap cyber crime menjadi kebutuhan penting dalam menjaga stabilitas dan keamanan ruang digital nasional.[15]

Negara melalui Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik berupaya memberikan perlindungan terhadap sistem elektronik dan kepentingan masyarakat di ruang digital. Regulasi tersebut dibentuk sebagai respons terhadap perkembangan teknologi informasi yang memunculkan berbagai bentuk kejahatan baru berbasis elektronik. Dalam Undang-Undang ITE diatur berbagai larangan terhadap tindakan yang dapat mengganggu keamanan sistem elektronik, seperti akses ilegal, manipulasi data elektronik, penyebaran informasi palsu, dan intersepsi tanpa hak. Dengan adanya pengaturan tersebut, negara berupaya menciptakan ruang digital yang aman dan tertib bagi masyarakat.

Dalam perspektif teori negara hukum, keberadaan regulasi cyber crime menunjukkan bahwa negara memiliki kewajiban untuk menjaga ketertiban dan memberikan perlindungan hukum terhadap masyarakat. Konsep negara hukum menempatkan hukum sebagai dasar dalam mengatur kehidupan sosial, termasuk dalam penggunaan teknologi informasi. Oleh sebab itu, setiap aktivitas di ruang digital harus dilakukan berdasarkan ketentuan hukum yang berlaku agar tidak merugikan pihak lain. Pengaturan cyber crime menjadi instrumen penting dalam memastikan bahwa perkembangan teknologi tetap berjalan sesuai dengan prinsip-prinsip hukum dan keadilan.[16]

Pengaturan hukum terhadap cyber crime juga bertujuan memberikan kepastian hukum bagi masyarakat dalam penggunaan teknologi informasi. Kepastian hukum diperlukan agar masyarakat mengetahui batasan-batasan tindakan yang diperbolehkan dan yang dilarang dalam ruang digital. Dalam Pasal 30 Undang-Undang ITE ditegaskan bahwa setiap orang dilarang mengakses sistem elektronik milik pihak lain tanpa hak. Ketentuan tersebut memberikan kejelasan bahwa tindakan peretasan atau akses ilegal terhadap sistem elektronik merupakan tindak pidana yang dapat dikenai sanksi pidana. Dengan demikian, masyarakat memperoleh perlindungan hukum terhadap ancaman penyalahgunaan teknologi informasi.

Selain memberikan kepastian hukum, pengaturan cyber crime juga bertujuan menciptakan keamanan digital bagi masyarakat. Keamanan digital sangat penting karena sistem elektronik saat ini digunakan dalam berbagai aktivitas penting, seperti transaksi perbankan, pelayanan publik, dan penyimpanan data pribadi. Apabila keamanan sistem elektronik terganggu, maka dapat menimbulkan kerugian besar baik secara materiil maupun immateriil. Oleh sebab

[13] Peter Mahmud Marzuki, *Pengantar Ilmu Hukum*, Jakarta: Kencana, 2008, hlm. 235.
[14] Hans Kelsen, *Pure Theory of Law*, Berkeley: University of California Press, 1967, hlm. 195.
[15] Bambang Waluyo, *Penegakan Hukum di Indonesia*, Jakarta: Sinar Grafika, 2008, hlm. 91.
[16] Jimly Asshiddiqie, *Konstitusi dan Konstitusionalisme Indonesia*, Jakarta: Sinar Grafika, 2010, hlm. 56.

FAKULTAS HUKUM UNSRAT 2026

itu, pengaturan hukum cyber crime menjadi bagian dari upaya negara dalam menjaga keamanan nasional di bidang teknologi informasi.[17]

Pengaturan hukum cyber crime juga memiliki hubungan erat dengan perlindungan terhadap hak privasi masyarakat. Perkembangan teknologi digital menyebabkan banyak data pribadi masyarakat tersimpan dalam sistem elektronik yang rentan disalahgunakan. Tindakan pencurian dan penyebaran data pribadi tanpa izin merupakan salah satu bentuk cyber crime yang dapat merugikan masyarakat secara serius. Oleh sebab itu, negara perlu memastikan bahwa penggunaan data elektronik dilakukan sesuai dengan ketentuan hukum dan prinsip perlindungan hak asasi manusia.[18]

Selain perlindungan terhadap individu, pengaturan hukum cyber crime juga bertujuan menjaga stabilitas sistem elektronik milik pemerintah dan sektor publik. Sistem elektronik pemerintah menyimpan berbagai data strategis yang berkaitan dengan administrasi negara dan pelayanan masyarakat. Apabila sistem tersebut diretas atau disalahgunakan, maka dapat mengganggu keamanan negara dan kepercayaan publik terhadap pemerintah. Oleh sebab itu, pengaturan hukum terhadap cyber crime merupakan bagian penting dalam menjaga keamanan sistem informasi nasional dan mendukung tata kelola pemerintahan berbasis digital.

Dengan demikian, pengaturan hukum terhadap cyber crime pada akhirnya bertujuan menciptakan keamanan, ketertiban, dan kepastian hukum dalam penggunaan teknologi informasi. Melalui Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, negara berupaya memberikan perlindungan terhadap sistem elektronik serta kepentingan masyarakat di ruang digital. Pengaturan tersebut diharapkan mampu mendorong masyarakat menggunakan teknologi informasi secara aman, bertanggung jawab, dan sesuai dengan ketentuan hukum yang berlaku. Oleh sebab itu, keberadaan regulasi cyber crime menjadi sangat penting dalam menghadapi perkembangan teknologi digital dan tantangan kejahatan siber di era modern.[19]

[17] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Bandung: Refika Aditama, 2010, hlm. 143.
[18] Sutan Remy Sjahdeini, *Kejahatan dan Tindak Pidana Komputer*, Jakarta: Pustaka Utama Grafiti, 2009, hlm. 54.
[19] Lilik Mulyadi, *Kapita Selekta Hukum Pidana, Kriminologi dan Victimologi*, Jakarta: Djambatan, 2007, hlm. 118.

B. Penegakan Hukum Tindak Pidana Cyber Crime Ditinjau Dari Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Transaksi Elektronik

Penegakan hukum terhadap tindak pidana cyber crime merupakan bagian penting dalam menjaga keamanan dan ketertiban masyarakat di era digital. Perkembangan teknologi informasi yang semakin pesat menyebabkan ruang siber menjadi sarana baru bagi terjadinya berbagai bentuk kejahatan. Cyber crime tidak hanya merugikan individu secara materiil, tetapi juga dapat mengganggu stabilitas sistem elektronik negara dan keamanan data masyarakat. Oleh sebab itu, negara melalui Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik berupaya memperkuat sistem penegakan hukum terhadap kejahatan siber. Penegakan hukum tersebut bertujuan memberikan perlindungan hukum sekaligus menciptakan kepastian hukum dalam penggunaan teknologi informasi.[20]

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik menjadi dasar hukum utama dalam penegakan tindak pidana cyber crime di Indonesia. Undang-undang tersebut mengatur berbagai bentuk perbuatan yang dilarang dalam penggunaan sistem elektronik, seperti akses ilegal, manipulasi data elektronik, intersepsi tanpa hak, dan penyebaran informasi elektronik yang melanggar hukum. Pengaturan tersebut menunjukkan bahwa negara memberikan perhatian serius terhadap perlindungan keamanan digital nasional. Dengan demikian, penegakan hukum cyber crime tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada perlindungan masyarakat dan sistem elektronik

Dalam Pasal 30 Undang-Undang ITE ditegaskan bahwa setiap orang dilarang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain. Ketentuan tersebut menjadi dasar hukum terhadap tindakan peretasan (*hacking*) yang sering terjadi dalam praktik cyber crime. Selain itu, Pasal 32 Undang-Undang ITE juga melarang tindakan mengubah, memindahkan, merusak, atau menyembunyikan informasi elektronik milik pihak lain tanpa hak. Oleh sebab itu, penegakan hukum terhadap cyber crime dilakukan melalui penerapan norma pidana yang secara khusus mengatur penggunaan teknologi informasi.

[20] Satjipto Rahardjo, Op.Cit, hlm. 220.

FAKULTAS HUKUM UNSRAT

Penegakan hukum cyber crime juga berkaitan erat dengan pengakuan alat bukti elektronik dalam sistem hukum pidana Indonesia. Pasal 5 Undang-Undang ITE menyatakan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang sah. Ketentuan ini sangat penting karena tindak pidana cyber crime pada umumnya meninggalkan jejak digital yang hanya dapat dibuktikan melalui alat bukti elektronik. Dengan demikian, hukum acara pidana di Indonesia telah menyesuaikan diri dengan perkembangan teknologi informasi modern.

Dalam praktik penegakan hukum cyber crime, aparat penegak hukum memiliki tanggung jawab besar untuk melakukan penyelidikan dan penyidikan terhadap tindak pidana siber. Penyidik harus memahami mekanisme kerja sistem elektronik, jaringan internet, dan teknik digital forensik untuk mengungkap pelaku kejahatan siber. Oleh sebab itu, peningkatan kualitas sumber daya manusia aparat penegak hukum menjadi faktor penting dalam efektivitas penegakan hukum cyber crime di Indonesia.[21]

Seperti contoh kasus yakni Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr yang berkaitan dengan tindak pidana akses ilegal terhadap sistem elektronik pemerintah daerah. Dalam perkara tersebut, terdakwa melakukan akses tanpa hak terhadap situs *sitepak.bekasikab.go.id* untuk memperoleh dokumen elektronik tertentu. Tindakan tersebut dilakukan dengan menggunakan perangkat komputer dan jaringan internet tanpa izin resmi dari pihak yang berwenang. Kasus ini menunjukkan bahwa cyber crime dapat mengancam keamanan sistem elektronik pemerintahan apabila tidak diimbangi dengan sistem keamanan digital yang memadai.

Dalam pertimbangan hukumnya, majelis hakim menyatakan bahwa terdakwa telah memenuhi unsur tindak pidana sebagaimana diatur dalam Pasal 30 ayat (2) jo. Pasal 46 ayat (2) Undang-Undang ITE. Hakim menilai bahwa tindakan mengakses sistem elektronik milik pihak lain tanpa hak merupakan bentuk perbuatan melawan hukum yang dapat dipidana. Pertimbangan tersebut menunjukkan bahwa Undang-Undang ITE telah memberikan dasar hukum yang jelas dalam penegakan hukum cyber crime di Indonesia. Dengan demikian, pengadilan memiliki landasan normatif yang kuat dalam menjatuhkan sanksi pidana terhadap pelaku kejahatan siber.

[21] Peter Mahmud Marzuki, Op.Cit, hlm. 200.

Kasus Putusan Pengadilan Negeri Cikarang tersebut juga memperlihatkan pentingnya alat bukti elektronik dalam proses pembuktian perkara cyber crime. Dalam perkara tersebut, hakim mempertimbangkan bukti berupa data elektronik, log akses sistem, serta hasil pemeriksaan digital forensik untuk membuktikan adanya tindak pidana akses ilegal. Hal ini menunjukkan bahwa perkembangan teknologi informasi menyebabkan sistem pembuktian hukum pidana juga mengalami perkembangan yang signifikan. Oleh sebab itu, penguasaan teknologi digital menjadi kebutuhan utama dalam penegakan hukum cyber crime.

Penegakan hukum cyber crime juga memiliki hubungan erat dengan perlindungan terhadap data pribadi masyarakat. Perkembangan teknologi informasi menyebabkan berbagai data pribadi tersimpan dalam sistem elektronik yang rentan disalahgunakan. Tindakan pencurian dan penyalahgunaan data pribadi merupakan salah satu bentuk cyber crime yang sering terjadi di era digital. Oleh karena itu, penegakan hukum terhadap cyber crime juga bertujuan melindungi hak privasi masyarakat sebagai bagian dari hak asasi manusia.[22]

Dalam praktiknya, penegakan hukum terhadap cyber crime menghadapi berbagai kendala, salah satunya adalah sifat kejahatan siber yang lintas negara (*transnational crime*). Pelaku cyber crime dapat melakukan tindak pidana dari wilayah negara lain melalui jaringan internet global. Kondisi tersebut menyebabkan aparat penegak hukum memerlukan kerja sama internasional dalam melakukan penyelidikan dan penindakan terhadap pelaku cyber crime. Oleh sebab itu, penegakan hukum cyber crime membutuhkan harmonisasi hukum nasional dan internasional.[23]

Selain itu, perkembangan teknologi yang sangat cepat menyebabkan bentuk-bentuk cyber crime terus mengalami perubahan. Modus operandi pelaku kejahatan siber semakin kompleks dan sulit dideteksi dengan metode konvensional. Oleh sebab itu, aparat penegak hukum harus terus meningkatkan kemampuan dan teknologi yang dimiliki agar mampu mengikuti perkembangan bentuk-bentuk cyber crime modern. Penegakan hukum yang tidak didukung oleh perkembangan teknologi akan mengalami kesulitan dalam mengungkap tindak pidana siber.

[22] Edmon Makarim, Op.Cit, hlm. 135.

[23] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*, Jakarta: Kencana, 2011, hlm. 54.

FAKULTAS HUKUM UNSRAT 2026

Dalam perspektif sosiologi hukum, penegakan hukum cyber crime menunjukkan bahwa hukum harus mampu beradaptasi dengan perubahan sosial dan teknologi masyarakat. Kemajuan teknologi digital menciptakan bentuk-bentuk hubungan hukum baru yang sebelumnya tidak dikenal dalam hukum konvensional. Oleh sebab itu, pembentukan Undang-Undang ITE merupakan bentuk respons negara terhadap perkembangan teknologi informasi dan meningkatnya ancaman cyber crime di Indonesia.[24]

Penegakan hukum cyber crime juga berkaitan dengan perlindungan terhadap kepentingan negara dan keamanan nasional. Sistem elektronik pemerintah mengandung berbagai data strategis yang berkaitan dengan administrasi negara dan pelayanan publik. Apabila sistem elektronik tersebut diretas atau disalahgunakan, maka dapat mengganggu stabilitas pemerintahan dan keamanan nasional. Oleh sebab itu, penegakan hukum terhadap cyber crime memiliki fungsi penting dalam menjaga keamanan digital negara.

Kasus Putusan Pengadilan Negeri Cikarang menunjukkan bahwa tindak pidana cyber crime tidak hanya menyerang individu, tetapi juga dapat menyerang sistem elektronik milik pemerintah. Tindakan akses ilegal terhadap sistem pemerintah dapat menyebabkan kebocoran data dan gangguan pelayanan publik. Oleh karena itu, penegakan hukum terhadap cyber crime harus dilakukan secara tegas untuk memberikan efek jera kepada pelaku dan menjaga keamanan sistem elektronik nasional.

Dalam sistem hukum pidana Indonesia, penegakan hukum terhadap cyber crime tidak hanya dilakukan melalui pemidanaan, tetapi juga melalui upaya pencegahan (*preventif*). Upaya preventif dilakukan melalui peningkatan keamanan sistem elektronik, edukasi masyarakat mengenai keamanan digital, dan penguatan pengawasan terhadap penggunaan teknologi informasi. Dengan demikian, penanggulangan cyber crime tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada pencegahan terjadinya kejahatan siber.[25]

Selain upaya preventif, penegakan hukum cyber crime juga dilakukan melalui upaya represif berupa penyidikan, penuntutan, dan pemidanaan terhadap pelaku tindak pidana siber. Penegakan hukum represif bertujuan memberikan sanksi kepada pelaku yang terbukti melakukan cyber crime sesuai dengan ketentuan peraturan perundang-undangan. Oleh sebab itu, proses peradilan pidana memiliki peranan penting dalam mewujudkan keadilan dan kepastian hukum terhadap tindak pidana cyber crime.

Perkembangan teknologi informasi juga menyebabkan masyarakat semakin bergantung pada sistem elektronik dalam berbagai aktivitas sehari-hari. Ketergantungan tersebut meningkatkan risiko terjadinya cyber crime yang dapat merugikan masyarakat secara luas. Oleh sebab itu, penegakan hukum cyber crime menjadi kebutuhan mendesak untuk menjaga keamanan dan kepercayaan masyarakat terhadap penggunaan teknologi digital.[26]

Penguatan penegakan hukum cyber crime juga harus didukung oleh peningkatan kesadaran hukum masyarakat mengenai penggunaan teknologi informasi secara bertanggung jawab. Masyarakat perlu memahami bahwa penggunaan sistem elektronik harus dilakukan sesuai dengan norma hukum yang berlaku. Kesadaran hukum tersebut penting untuk mencegah masyarakat terlibat dalam tindak pidana siber maupun menjadi korban cyber crime.[27]

Kesadaran hukum merupakan faktor penting dalam menciptakan ketertiban dan keamanan dalam penggunaan sistem elektronik di era digital. Masyarakat perlu memahami bahwa perkembangan teknologi informasi tidak hanya memberikan manfaat, tetapi juga menimbulkan risiko hukum apabila digunakan secara tidak tepat. Oleh sebab itu, penggunaan media elektronik harus dilakukan sesuai dengan norma hukum dan etika sosial yang berlaku. Dengan adanya kesadaran hukum yang baik, masyarakat dapat lebih berhati-hati dalam menggunakan teknologi informasi serta menghindari perbuatan yang dapat menimbulkan pelanggaran hukum.

Kesadaran hukum masyarakat terhadap penggunaan teknologi informasi menjadi semakin penting karena perkembangan internet telah mengubah pola komunikasi dan aktivitas sosial masyarakat modern. Hampir seluruh aktivitas kehidupan saat ini bergantung pada sistem elektronik, mulai dari transaksi ekonomi, pendidikan, pemerintahan, hingga komunikasi pribadi. Kondisi tersebut menyebabkan ruang digital menjadi bagian penting dalam kehidupan masyarakat. Namun demikian, tidak seluruh

[24] Soerjono Soekanto, *Pokok-Pokok Sosiologi Hukum*, Jakarta: Raja Grafindo Persada, 2006, hlm. 38.
[25] Sudikno Mertokusumo, *Mengenal Hukum: Suatu Pengantar*, Yogyakarta: Liberty, 2011, hlm. 126.
[26] Munir Fuady, *Hukum Bisnis dalam Teori dan Praktik*, Bandung: Citra Aditya Bakti, 2014, hlm. 201.
[27] Soerjono Soekanto, *Kesadaran Hukum dan Kepatuhan Hukum*, Jakarta: Rajawali Pers, 1982, hlm. 152.

FAKULTAS HUKUM UNSRAT 2026

masyarakat memahami batasan hukum dalam penggunaan teknologi informasi sehingga sering terjadi pelanggaran hukum yang dilakukan tanpa kesadaran penuh. Oleh sebab itu, edukasi hukum digital menjadi kebutuhan penting dalam masyarakat modern.

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik telah memberikan dasar hukum yang jelas mengenai larangan berbagai bentuk penyalahgunaan teknologi informasi. Dalam Pasal 30 Undang-Undang ITE ditegaskan bahwa setiap orang dilarang mengakses sistem elektronik milik pihak lain tanpa hak. Selain itu, Pasal 32 juga melarang tindakan memindahkan, mengubah, merusak, atau menyembunyikan informasi elektronik milik orang lain secara melawan hukum. Ketentuan tersebut menunjukkan bahwa penggunaan teknologi informasi harus dilakukan secara bertanggung jawab dan sesuai dengan norma hukum yang berlaku.

Kesadaran hukum masyarakat juga penting untuk mencegah masyarakat menjadi korban cyber crime. Banyak kasus kejahatan siber terjadi akibat rendahnya pemahaman masyarakat terhadap keamanan digital, seperti penggunaan kata sandi yang lemah, penyebaran data pribadi secara sembarangan, atau mudah percaya terhadap informasi palsu di internet. Kondisi tersebut menyebabkan pelaku cyber crime lebih mudah melakukan tindakan penipuan maupun pencurian data elektronik. Oleh sebab itu, edukasi mengenai keamanan digital harus dilakukan secara berkelanjutan oleh pemerintah dan lembaga terkait.[28]

Peningkatan kesadaran hukum masyarakat terhadap cyber crime juga berkaitan dengan perkembangan budaya hukum di era digital. Budaya hukum merupakan sikap dan perilaku masyarakat terhadap hukum dalam kehidupan sehari-hari. Dalam konteks teknologi informasi, budaya hukum digital dapat diwujudkan melalui penggunaan media elektronik secara etis, bertanggung jawab, dan menghormati hak-hak orang lain. Oleh sebab itu, pembentukan budaya hukum digital menjadi bagian penting dalam menciptakan ruang siber yang aman dan tertib.

Negara memiliki tanggung jawab untuk meningkatkan kesadaran hukum masyarakat melalui pendidikan dan sosialisasi hukum digital. Pemerintah dapat melakukan edukasi melalui lembaga pendidikan, media sosial, seminar, maupun program literasi digital nasional. Selain itu, aparat penegak hukum juga perlu memberikan pemahaman kepada masyarakat mengenai risiko hukum dari penggunaan teknologi informasi yang melanggar hukum. Dengan demikian, masyarakat dapat lebih memahami pentingnya menjaga keamanan dan etika dalam penggunaan sistem elektronik.

Tanggung jawab tersebut merupakan bagian dari fungsi negara dalam memberikan perlindungan hukum kepada masyarakat di era perkembangan teknologi informasi. Kemajuan teknologi digital telah membawa perubahan besar dalam pola kehidupan masyarakat, sehingga penggunaan sistem elektronik menjadi bagian penting dalam aktivitas sehari-hari. Namun demikian, perkembangan tersebut juga meningkatkan risiko terjadinya penyalahgunaan teknologi informasi dan tindak pidana cyber crime. Oleh sebab itu, negara harus hadir untuk memberikan edukasi hukum agar masyarakat memahami penggunaan teknologi informasi secara aman dan bertanggung jawab.

Dalam perspektif negara hukum, pemerintah memiliki kewajiban untuk menciptakan ketertiban dan keamanan dalam penggunaan teknologi informasi. Konsep negara hukum sebagaimana diatur dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menegaskan bahwa segala tindakan masyarakat dan pemerintah harus didasarkan pada hukum. Ketentuan tersebut menunjukkan bahwa penggunaan teknologi informasi juga harus tunduk pada norma hukum yang berlaku. Dengan demikian, negara memiliki peranan penting dalam membentuk budaya hukum digital melalui pendidikan dan sosialisasi hukum kepada masyarakat.

Pendidikan hukum digital menjadi sangat penting karena perkembangan teknologi informasi telah menciptakan bentuk-bentuk hubungan hukum baru dalam masyarakat. Banyak masyarakat yang menggunakan media sosial, sistem elektronik, dan internet tanpa memahami risiko hukum dari tindakan yang dilakukan di ruang digital. Kondisi tersebut menyebabkan masih sering terjadi pelanggaran hukum seperti penyebaran hoaks, pencemaran nama baik digital, penipuan online, hingga akses ilegal terhadap sistem elektronik. Oleh sebab itu, pendidikan hukum digital diperlukan untuk meningkatkan pemahaman masyarakat terhadap batasan hukum dalam penggunaan teknologi informasi.[29]

[28] Edmon Makarim, *Pengantar Hukum Telematika*, Jakarta: Raja Grafindo Persada, 2005, hlm. 112.

[29] Edmon Makarim, *Pengantar Hukum Telematika*, Op.Cit, hlm. 231.

Pemerintah dapat melakukan sosialisasi hukum digital melalui lembaga pendidikan formal maupun nonformal. Pendidikan mengenai etika dan hukum penggunaan teknologi informasi dapat dimasukkan dalam kurikulum sekolah maupun perguruan tinggi. Selain itu, pemerintah juga dapat bekerja sama dengan lembaga masyarakat dan media massa dalam memberikan edukasi mengenai keamanan digital. Langkah tersebut penting untuk membentuk kesadaran hukum sejak dini agar masyarakat lebih bijak dalam menggunakan teknologi informasi. Selain melalui lembaga pendidikan, sosialisasi hukum digital juga dapat dilakukan melalui media sosial dan platform digital yang banyak digunakan masyarakat. Penggunaan media sosial sebagai sarana edukasi hukum menjadi sangat efektif karena mampu menjangkau masyarakat secara luas dan cepat. Pemerintah dapat menyampaikan informasi mengenai bentuk-bentuk cyber crime, ancaman hukum, serta cara penggunaan teknologi informasi yang aman melalui berbagai platform digital. Dengan demikian, masyarakat dapat lebih mudah memahami pentingnya menjaga keamanan dan etika dalam penggunaan sistem elektronik.[30]

Peningkatan kesadaran hukum masyarakat juga berkaitan dengan upaya perlindungan terhadap korban cyber crime. Banyak masyarakat menjadi korban tindak pidana siber akibat kurangnya pemahaman mengenai keamanan digital, seperti mudah memberikan data pribadi atau percaya terhadap informasi palsu di internet. Kondisi tersebut dimanfaatkan oleh pelaku cyber crime untuk melakukan penipuan, pencurian data, maupun tindakan ilegal lainnya. Oleh sebab itu, edukasi hukum digital tidak hanya bertujuan mencegah masyarakat menjadi pelaku cyber crime, tetapi juga melindungi masyarakat agar tidak menjadi korban kejahatan siber.

Dengan demikian, negara memiliki peranan yang sangat penting dalam meningkatkan kesadaran hukum masyarakat mengenai penggunaan teknologi informasi secara bertanggung jawab. Pendidikan dan sosialisasi hukum digital harus dilakukan secara berkelanjutan melalui lembaga pendidikan, media sosial, seminar, dan program literasi digital nasional. Aparat penegak hukum juga perlu aktif memberikan pemahaman kepada masyarakat mengenai risiko hukum dari penyalahgunaan teknologi informasi. Melalui peningkatan kesadaran hukum tersebut, masyarakat diharapkan mampu menggunakan sistem elektronik secara aman, etis, dan sesuai dengan ketentuan hukum yang berlaku sehingga dapat meminimalkan terjadinya tindak pidana cyber crime di Indonesia.

Perkembangan teknologi informasi yang sangat cepat menyebabkan bentuk-bentuk cyber crime juga terus berkembang. Pelaku cyber crime memanfaatkan rendahnya pemahaman masyarakat terhadap teknologi digital untuk melakukan berbagai tindak pidana, seperti *phishing*, *hacking*, pencurian identitas, dan penipuan online. Oleh sebab itu, peningkatan kesadaran hukum masyarakat harus diimbangi dengan peningkatan kemampuan literasi digital agar masyarakat mampu mengenali berbagai bentuk ancaman siber. Kesadaran hukum dan literasi digital merupakan dua hal yang saling berkaitan dalam upaya pencegahan cyber crime.[31]

Dengan demikian, penguatan penegakan hukum cyber crime tidak hanya bergantung pada keberadaan peraturan perundang-undangan dan aparat penegak hukum, tetapi juga sangat dipengaruhi oleh tingkat kesadaran hukum masyarakat. Masyarakat yang memahami norma hukum dan etika digital akan lebih mampu menggunakan teknologi informasi secara bertanggung jawab dan aman. Kesadaran hukum tersebut penting untuk mencegah masyarakat terlibat dalam tindak pidana siber maupun menjadi korban cyber crime. Oleh sebab itu, peningkatan edukasi hukum dan literasi digital harus terus dilakukan sebagai bagian dari upaya menciptakan keamanan dan ketertiban dalam ruang siber di Indonesia.

Penegakan hukum tindak pidana cyber crime ditinjau dari Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik merupakan upaya negara dalam menjaga keamanan ruang digital nasional. Penegakan hukum tersebut dilakukan melalui pengaturan norma pidana, pengakuan alat bukti elektronik, peningkatan kapasitas aparat penegak hukum, dan penerapan sanksi pidana terhadap pelaku cyber crime. Kasus Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr menjadi contoh nyata penerapan penegakan hukum terhadap tindak pidana akses ilegal sistem elektronik di Indonesia.

Efektivitas penegakan hukum cyber crime sangat bergantung pada sinergi antara regulasi hukum, aparat penegak hukum, teknologi keamanan digital, dan kesadaran hukum masyarakat. Negara harus terus memperkuat

[30] Munir Fuady, *Hukum Bisnis dalam Teori dan Praktik*, Bandung: Citra Aditya Bakti, 2014, hlm. 212.

[31] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*, Jakarta: Kencana, 2011, hlm. 54.

sistem hukum dan keamanan siber untuk menghadapi perkembangan kejahatan digital yang semakin kompleks. Dengan penegakan hukum yang efektif, penggunaan teknologi informasi di Indonesia diharapkan dapat berlangsung secara aman, tertib, dan memberikan manfaat bagi masyarakat luas.[32]

PENUTUP

A. Kesimpulan

1. Berdasarkan pembahasan mengenai faktor penyebab terjadinya cyber crime, dapat disimpulkan bahwa kejahatan siber merupakan fenomena yang kompleks dan dipengaruhi oleh berbagai faktor yang saling berkaitan. Faktor utama yang mendorong terjadinya cyber crime meliputi perkembangan teknologi yang pesat tanpa diimbangi dengan sistem keamanan yang memadai, faktor ekonomi yang memotivasi pelaku untuk memperoleh keuntungan secara instan, serta rendahnya kesadaran hukum dan literasi digital masyarakat. Selain itu, faktor sosial dan psikologis seperti anonimitas di dunia maya dan dorongan untuk menguji kemampuan juga turut berkontribusi terhadap meningkatnya kejahatan siber. Lemahnya pengawasan serta keterbatasan kapasitas aparat penegak hukum juga menjadi faktor pendukung yang memperbesar peluang terjadinya cyber crime. Dengan demikian, cyber crime tidak hanya merupakan persoalan hukum semata, tetapi juga berkaitan dengan aspek teknologi, sosial, dan budaya masyarakat.
2. Dalam hal penanggulangan tindak pidana cyber crime ditinjau dari Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, dapat disimpulkan bahwa regulasi tersebut telah memberikan dasar hukum yang cukup komprehensif dalam menangani kejahatan siber di Indonesia. Undang-undang ini mengatur berbagai bentuk perbuatan yang dilarang serta memberikan sanksi pidana yang tegas bagi pelaku cyber crime. Namun, efektivitas penanggulangan tidak hanya bergantung pada keberadaan norma hukum, melainkan juga pada implementasi yang didukung oleh koordinasi antar lembaga penegak hukum, peningkatan kapasitas sumber daya manusia, serta partisipasi aktif masyarakat dan sektor swasta. Penanggulangan cyber crime juga harus dilakukan secara terpadu melalui pendekatan preventif, represif, dan edukatif. Oleh karena itu, keberhasilan penegakan hukum di bidang siber sangat ditentukan oleh sinergi antara berbagai pihak serta kemampuan adaptasi hukum terhadap perkembangan teknologi.

B. Saran

1. Pemerintah dan pembentuk undang-undang disarankan untuk terus melakukan pembaruan dan penyempurnaan terhadap regulasi di bidang teknologi informasi, khususnya Undang-Undang Nomor 1 Tahun 2024, agar tetap relevan dengan perkembangan teknologi yang sangat dinamis. Selain itu, perlu segera disusun peraturan pelaksana yang lebih teknis dan operasional guna mendukung implementasi undang-undang tersebut di lapangan. Penguatan koordinasi antar lembaga penegak hukum, seperti kepolisian, kejaksaan, dan pengadilan, juga perlu ditingkatkan agar penanganan perkara cyber crime dapat dilakukan secara efektif dan efisien. Di samping itu, pemerintah perlu meningkatkan investasi dalam pengembangan infrastruktur keamanan siber nasional serta pelatihan khusus bagi aparat penegak hukum di bidang forensik digital.
2. Masyarakat dan sektor swasta disarankan untuk lebih aktif dalam mendukung upaya penanggulangan cyber crime melalui peningkatan kesadaran dan literasi digital. Perusahaan yang mengelola data pengguna harus menerapkan standar keamanan yang tinggi serta bertanggung jawab dalam melindungi data pribadi pengguna dari potensi kebocoran. Selain itu, masyarakat perlu lebih berhati-hati dalam menggunakan teknologi informasi serta tidak mudah terpengaruh oleh berbagai modus kejahatan siber seperti penipuan daring. Edukasi yang berkelanjutan mengenai keamanan siber perlu terus dilakukan oleh pemerintah, lembaga pendidikan, dan sektor swasta. Dengan adanya peran aktif dari seluruh elemen masyarakat, diharapkan upaya penanggulangan cyber crime dapat berjalan secara optimal dan berkelanjutan.

DAFTAR PUSTAKA

Buku-Buku

Arief, Barda Nawawi, *Bunga Rampai Kebijakan Hukum Pidana*, Jakarta: Prenadamedia Group, 2018.

[32] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat Indonesia*, Surabaya: Bina Ilmu, 2007, hlm. 65.

FAKULTAS HUKUM UNSRAT 2026

_____, *Kebijakan Hukum Pidana dalam Era Digitalisasi*, Jakarta: Kencana, 2020.
_____, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Hukum Pidana*, Yogyakarta: Genta Publishing, 2017.
_____, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*, Jakarta: Kencana, 2011.
Asshiddiqie, Jimly, *Konstitusi dan Konstitusionalisme Indonesia*, Jakarta: Sinar Grafika, 2019.
Atmasasmita, Romli, *Reformasi Hukum, Hak Asasi Manusia, dan Penegakan Hukum*, Bandung: Mandar Maju, 2019.
_____, *Sistem Peradilan Pidana Kontemporer*, Jakarta: Kencana, 2010.
_____, *Teori Hukum Integratif*, Bandung: Genta Publishing, 2012.
Effendy, Marwan, *Perkembangan Hukum Pidana dan Kriminologi*, Bandung: Refika Aditama, 2020.
Friedman, Lawrence M., *The Legal System: A Social Science Perspective*, New York: Russell Sage Foundation, 1975.
Fuady, Munir, *Hukum Bisnis dalam Teori dan Praktik*, Bandung: Citra Aditya Bakti, 2014.
_____, *Hukum Telematika*, Bandung: Citra Aditya Bakti, 2005.
Hadjon, Philipus M., *Perlindungan Hukum bagi Rakyat Indonesia*, Surabaya: Bina Ilmu, 2007.
Hamzah, Andi, *Aspek-Aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika, 1992.
_____, *Delik-Delik Tertentu di Luar KUHP*, Jakarta: Rajawali Pers, 2022.
Kaelan, *Pancasila: Kajian Historis, Filosofis, dan Yuridis Kenegaraan*, Yogyakarta: Paradigma, 2016.
Kelsen, Hans, *Pure Theory of Law*, Berkeley: University of California Press, 1967.
Labib, Mohammad dkk, *Kejahatan Mayantara (Cyber Crime)*, Bandung: Refika Aditama, 2010.
Makarim, Edmon, *Pengantar Hukum Telematika*, Jakarta: Raja Grafindo Persada, 2005.
Mahrus Ali, *Hukum Pidana Umum*, Yogyakarta: UII Press, 2020.
Marzuki, Peter Mahmud, *Pengantar Ilmu Hukum*, Jakarta: Kencana, 2008.
_____, *Penelitian Hukum*, Jakarta: Kencana Prenada Media Group, 2008.
Mertokusumo, Sudikno, *Mengenal Hukum: Suatu Pengantar*, Yogyakarta: Liberty, 2011.
Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2008.
Muladi, *Kebijakan Kriminal dalam Penanggulangan Kejahatan*, Bandung: Alumni, 2019.
Muladi dan Barda Nawawi Arief, *Teori dan Kebijakan Pidana*, Bandung: Alumni, 2018.
Muliadi, Ahmad dkk, *Metode Penulisan*, Jakarta: Universitas Jayabaya, 2016.
Poerwadarminta, W.J.S., *Kamus Umum Bahasa Indonesia*, Jakarta: Balai Pustaka, 2003.
Radbruch, Gustav, *Legal Philosophy*, London: Oxford University Press, 1950.
Rahardjo, Satjipto, *Hukum Progresif: Sebuah Sintesa Hukum Indonesia*, Yogyakarta: Genta Publishing, 2009.
_____, *Ilmu Hukum*, Bandung: Citra Aditya Bakti, 2012.
_____, *Masalah Penegakan Hukum*, Bandung: Sinar Baru, 1983.
Ramli, Ahmad M., *Cyber Law dan Forensik Digital*, Bandung: Refika Aditama, 2021.
_____, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Bandung: Refika Aditama, 2010.
Soekanto, Soerjono, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Jakarta: Raja Grafindo Persada, 2010.
_____, *Kesadaran Hukum dan Kepatuhan Hukum*, Jakarta: Rajawali Pers, 1982.
_____, *Pengantar Penelitian Hukum*, Jakarta: UI Press, 1989.
_____, *Pokok-Pokok Sosiologi Hukum*, Jakarta: Raja Grafindo Persada, 2006.
Soekanto, Soerjono dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Jakarta: RajaGrafindo Persada, 2012.
Soemitro, Ronny Hanitijo, *Metodologi Penelitian Hukum dan Jurimetri*, Jakarta: Ghalia Indonesia, 1990.
Subagyo, P. Joko, *Metode Penelitian dalam Teori dan Praktik*, Jakarta: Rineka Cipta, 2011.
Sjahdeini, Sutan Remy, *Kejahatan dan Tindak Pidana Komputer*, Jakarta: Pustaka Utama Grafiti, 2009.
Waluyo, Bambang, *Penegakan Hukum di Indonesia*, Jakarta: Sinar Grafika, 2008.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
Kitab Undang-Undang Hukum Pidana (KUHP)
Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Terbaru)

FAKULTAS HUKUM UNSRAT 2026

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru)
Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP)
Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE
Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)
Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)
Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr

Jurnal/Publikasi/Lembaga

Interpol. *Cybercrime: Threats and Responses*. Lyon: Interpol General Secretariat, 2018.
Kementerian Komunikasi dan Informatika RI. *Naskah Akademik Perubahan UU ITE*. Jakarta, 2023.
United Nations Office on Drugs and Crime (UNODC). *Comprehensive Study on Cybercrime*. Vienna: United Nations Publication, 2013.
UNCITRAL. *Model Law on Electronic Commerce*. New York: United Nations, 1996.
Council of Europe. *Budapest Convention on Cybercrime*. Strasbourg: Council of Europe Publishing, 2001.
Oxford University Press. *Oxford English Dictionary*. Oxford: OUP, 2019.
Kamus Besar Bahasa Indonesia (KBBI). Edisi V. Jakarta: Badan Pengembangan dan Pembinaan Bahasa, 2021.

FAKULTAS HUKUM UNSRAT 2026