Indonesian Journal of Law

Vol. 1, No. 12, Desember 2024
Hal 312-320

E-ISSN: 3032-3622
P-ISSN: 3032-3614

Site: https://jurnal.intekom.id/index.php/inlaw

Perkembangan Teknologi Dan Tantangan Hukum Dalam Penanganan Kejahatan Mayantara: Perspektif Hukum Pidana Dan Perlindungan Data Pribadi Di Indonesia

Ahmad Fauzi M[1], Amelia Komalasari[2], Brahmantika Satria[3], Fatimah Zahra R. N[4], Ria Anggraeni Utami[5]

[1,2,3,4,5]Fakultas Hukum, Universitas Bengkulu, Bengkulu, Indonesia

Article Info

Article history:

Received Desember 15, 2024
Revised Desember 15, 2024
Accepted Desember 19, 2024

Kata Kunci:

Kejahatan Mayantara,
Teknologi Informasi,
Hukum Pidana

Keywords:

Cybercrime,
Information Technology,
Criminal Law

ABSTRAK

Tantangan yang dihadapi oleh hukum pidana dalam menanggapi perkembangan teknologi terkait kejahatan mayantara (cybercrime) di Indonesia dikarenakan perkembangan teknologi yang pesat, terutama di bidang kejahatan mayantara, terdapat beberapa kasus yang menggambarkan kompleksitas penanganan kejahatan mayantara, seperti kasus peretasan data pribadi oleh Bjorka. Meskipun telah dikeluarkan undang-undang perlindungan data pribadi, masih banyak kebocoran data yang terjadi, yang akhirnya menimbulkan kekhawatiran di masyarakat. Literasi teknologi yang meningkat juga menjadi sasaran empuk bagi oknum-oknum yang melakukan kejahatan mayantara di indoneisa. Hukum pidana yang harus terus mengikuti perkembangan kejahatan sehingga dapat memastikan kepastian, keadilan, dan kemanfaatan hukum terkait kejahatan mayantara di Indonesia, bentuk-bentuk *cybercrime* yang umumnya dikenal telah ada dalam berbagai macam bentuk, dengan itu telah muncul kendala-kendala dalam penanggulangan kejahatan mayantara di Indonesia, upaya hukum pidana dalam menangani permasalahan ini terus dilakukan, seperti merumuskan pasal-pasal dalam undang-undang terbaru seperti Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

ABSTRACT

The challenges faced by criminal law in responding to technological developments related to cybercrime in Indonesia are due to rapid technological developments, especially in the field of cybercrime, there are several cases that illustrate the complexity of handling cybercrime, such as the case of personal data hacking by Bjorka. Although a personal data protection law has been issued, there are still many data leaks that occur, which ultimately raise concerns in the community. Increasing technological literacy is also an easy target for individuals who commit cybercrime in Indonesia. Criminal law must continue to follow the development of crime so that it can ensure certainty, justice, and legal benefits related to cybercrime in Indonesia, the forms of cybercrime that are generally known have existed in various forms, with that there have been obstacles in overcoming cybercrime in Indonesia, criminal law efforts to deal with this problem continue to be carried out, such as regulating articles in the latest laws such as Law Number 1 of 2023 concerning the Criminal Code.

Corresponding Author:

Ahmad Fauzi M
Fakultas Hukum, Universitas Bengkulu,
Bengkulu, Indonesia
Email: ameliakomala112@gmail.com

1. PENDAHULUAN

Perkembangan teknologi secara global yang begitu cepat menyebabkan perlunya hukum yang menurut Gustav Radbruch harus mengandung 3 (tiga) asas utama yaitu asas kepastian hukum, asas keadilan hukum dan asas kemanfaatan hukum, untuk memenuhi semua asas tersebut tentunya hukum harus ikut berkembang secara pesat juga demi memenuhi tindak pidana baru yang bermunculan seiring dengan perkembangan teknologi saat ini. Keberhasilan pembangunan nasional membutuhkan ketahanan nasional yang didukung oleh pemberdayaan masyarakat. Ketahanan ini merupakan kondisi di mana berbagai gangguan dan ancaman, termasuk yang berbentuk kejahatan, dapat dicegah atau diatasi dengan efektif [1]. Salah satu tindak pidana yang saat ini marak terjadi adalah Kejahatan Mayantara *(Cyber Crime)* yang lama kelamaan seiring berjalannya waktu cepat menyebar dan masuk ke sela-sela kehidupan masyarakat Indonesia Kejahatan Mayantara *(Cyber Crime)* ini memiliki dampak negatif yang sangat luas karena tidak ada batasan dalam melakukan Tindakan ini dikarenakan kejahatan-kejahatan ini banyak terjadi melalui internet yang tidak memiliki batas fisik sehingga bisa diakses oleh siapapun dan dimanapun.

Bertepatan Pada 17 Oktober 2022, Undang-undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi diundangkan, tentunya dengan Undang-undang ini pemerintah berharap bisa menanggulangi permasalahan kasus layaknya Bjorka ini, tetapi dalam kenyataannya masih banyak kebocoran data pribadi maupun korporasi (yang dimana seharusnya menjaga data tersebut agar tetap aman) terjadi, sehingga terdapat keresahan yang baru dalam masyarakat modern Indonesia terhadap data yang mereka miliki, Literasi teknologi yang semakin meningkat tentunya menjadi sasaran empuk bagi oknum-oknum yang menjadikan Mayantara/Internet sebagai ladang melakukan tindak kejahatan mereka, tantangan yang baru pula tentunya bagi Aparat Penegak Hukum dimana Penyidikan yang awalnya dibatasi oleh wilayah sekarang memiliki kendala yang lebih rumit karena internet yang bersifat *Borderless* dan Global, bahkan pada proses penuntutan ketika subjek yang melakukan tindakan kejahatan tersebut tidak diketahui maka Aparat Penegak Hukum akan memiliki kesulitan dalam melakukan proses penuntutan.

Salah satu contohnya adalah ketika terjadi fenomena dimana peretas *(hacker)* dari luar negeri dengan nama Bjorka melakukan tindakan peretasan yang membuat masyarakat khawatir, pasalnya Bjorka berhasil meretas 1,3 Miliar data registrasi kartu SIM masyarakat Indonesia, Bjorka menyatakan bahwa data yang berhasil diretas berasal dari Kementerian Komunikasi dan Informatika (Kominfo) dan dijual dengan harga US$500 ribu atau sekitar Rp745,6 juta. Data berukuran 87 GB tersebut berisi informasi seperti NIK, nomor ponsel, provider telekomunikasi, dan tanggal registrasi. Namun, hingga kini, sumber kebocoran data tersebut masih menjadi teka-teki. Kominfo sendiri mengklaim bahwa sampel data yang tersebar bukan berasal dari sistem mereka [2], dari kasus diatas dapat kita perhatikan betapa rumitnya gambaran penyelesaian kasus Kejahatan Mayantara *(Cyber Crime)* karena bahkan sampai saat ini

identitas dari Bjorka saja belum diketahui, sehingga salah satu unsur hukum pidana yang penting yaitu subjek tidak dapat dipenuhi sehingga hal yang bisa dilakukan Aparat Penegak Hukum Indonesia pada saat itu hanyalah memblokir akun-akun Bjorka dari media sosial .

Bertepatan Pada 17 Oktober 2022, Undang-undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi diundangkan, tentunya dengan Undang-undang ini pemerintah berharap bisa menanggulangi permasalahan kasus layaknya Bjorka ini, tetapi dalam kenyataannya masih banyak kebocoran data pribadi maupun korporasi (yang dimana seharusnya menjaga data tersebut agar tetap aman) terjadi, sehingga terdapat keresahan yang baru dalam masyarakat modern Indonesia terhadap data yang mereka miliki, Literasi teknologi yang semakin meningkat tentunya menjadi sasaran empuk bagi oknum-oknum yang menjadikan Mayantara/Internet sebagai ladang melakukan tindak kejahatan mereka, tantangan yang baru pula tentunya bagi Aparat Penegak Hukum dimana Penyidikan yang awalnya dibatasi oleh wilayah sekarang memiliki kendala yang lebih rumit karena internet yang bersifat *Borderless* dan Global, bahkan pada proses penuntutan ketika subjek yang melakukan tindakan kejahatan tersebut tidak diketahui maka Aparat Penegak Hukum akan memiliki kesulitan dalam melakukan proses penuntutan.

2. METODE

Penelitian ini menggunakan metode yuridis normatif untuk mengidentifikasi aturan hukum, prinsip, dan doktrin hukum yang relevan dalam menjawab permasalahan hukum yang sedang dianalisis . Penelitian atau kaidah hukum. Asas hukum dan doktrin hukum serta permasalahan yang dibahas dapat dijadikan sebagai jawaban untuk menjawab permasalahan yang akan dipecahkan atau diteliti. Metode ini didukung dengan 2 (dua) sumber bahan hukum yaitu bahan hukum primer yang bersifat sutoritatif dan memiliki otoritas dalam penelitian seperti peraturan perundang-undangan dan bahan hukum sekunder yang mendukung dan memperkuat bahan hukum primer sehingga dapat menganalisa secara mendalam seperti buku literatur, jurnal, hasil penelitian, dan sumber lain yang sesuai dengan topik pembahasan.

3. HASIL DAN PEMBAHASAN

3.1 Tantangan Hukum Pidana dalam menghadapi perkembangan teknologi terkait dengan Kejahatan Mayantara di Indonesia

Kejahatan Mayantara (*Cyber Crime)* yang tidak bisa lepas dari Kejahatan Komputer *(Computer Crime)* dikarenakan kedua kejahatan saling berhubungan erat dalam pelaksanaannya, kedua hubungan ini dapat juga dilihat dalam Pengertian yang dikemukakan oleh *The. U.S Department of Justice* yang memberikan pengertian Kejahatan Komputer *(Computer Crime)* sebagai berikut : *"...any illegal act requiring knowledge of computer technology for it's perpretation, investigation or prosecution"*[3] yang dapat diartikan sebagai : "tindakan ilegal apa pun yang memerlukan pengetahuan tentang teknologi komputer untuk melakukan, menyelidiki, atau melaksanakannya" pengertian lainnya yang diberikan oleh *Organization of European Community Development* yaitu : *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data"* [4] atau yang dapat diartikan sebagai : "segala perilaku ilegal, tidak etis, atau tidak sah terkait dengan pemrosesan otomatis dan/atau transmisi data" sehingga dapat terlihat bahwa korelasi antara Kejahatan Komputer dan Kejahatan Mayantara sangatlah dekat dan berhubungan, Andi

Hamzah dalam Bukunya Aspek-Aspek Pidana di Bidang Komputer (1989) menjelaskan bahwa : "Kejahatan di Bidang Komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal" [5]. Berdasarkan beberapa pengertian diatas dapat disimpulkan bahwa Kejahatan Komputer itu sendiri adalah Kejahatan dimana penggunaan komputer sebagai sarana/alat untuk melakukan tindakan kejahatan sedangkan Kejahatan Mayantara merupakan setiap tindakan atau perilaku yang melanggar hukum, etika, atau dilakukan tanpa kewenangan yang berkaitan dengan pemrosesan dan/atau pengiriman data. Umumnya, tindakan tersebut dilakukan menggunakan perangkat komputer atau sarana digital dalam ruang lingkup dunia maya (*cyber*).

Perluasan pengertian dari Kejahatan Mayantara *(Cyber Crime)* dapat dilakukan ketika memasukkan internet kedalam salah satu faktor pembantu untuk melakukan tindakan *Cyber Crime* tersebut, dimana Kejahatan Komputer dapat dilakukan tanpa internet seperti mengakses komputer orang lain tanpa izin dan menggunakan *Flashdisk* untuk mencuri data-data didalam komputer tersebut, sementara Kejahatan Mayantara *(Cyber Crime)* adalah kejahatan yang dapat dilakukan secara virtual dimana komputer tetap digunakan sebagai alat tetapi dengan adanya internet dapat meningkatkan derajat kejahatan dimana kejahatan dapat berkembang ke Negara lain yang berada di luar Yurisdiksi Negara tersebut [5], perbedaan yang mencolok dari contoh diatas adalah tindakan mengakses komputer seseorang tanpa izin hanya dibatasi oleh komputer seseorang tersebut, sedangkan jika komputer itu turut ikut serta tersambung ke Internet maka tingkat kejahatan dapat menjadi Internasional/Global karena internet tersebut, contoh yang awalnya hanya pencurian data pribadi menjadi penjualan data pribadi yang dapat disalahgunakan oleh oknum yang berasal dari berbagai macam Negara.

Peran hukum pidana sangat penting dalam menangani Kejahatan Mayantara (*Cyber Crime*), mengingat tindak pidana di ranah ini terus berkembang, baik dari segi kompleksitas maupun skala pelaksanaannya. Karena Cyber Crime adalah kejahatan yang dapat dilakukan tanpa batasan ruang dan waktu, diperlukan langkah-langkah pencegahan yang efektif untuk menanggulangi kejahatan tersebut [6]. Salah satu contohnya adalah penggabungan antara perdagangan anak dan perempuan dalam skala global dengan Pornografi, dimana terdapat pasar gelap yang memproduksi Pornografi anak *(Child Pornography)* yang semakin marak seperti yang diberitakan oleh *usatoday.com "The amount of child sex abuse material online has skyrocketed in the past five years, aided by the ubiquity of smartphones and the COVID-19 pandemic. According to the National Center for Missing and Exploited Children, monthly reports of such material doubled from about 1 million in March 2019 to 2 million a year later. Reports increased by an additional 35% from 2020 to 2021."* [7] atau yang dapat diartikan dengan "Jumlah materi pelecehan seksual terhadap anak secara online telah meroket dalam lima tahun terakhir, hal ini disebabkan oleh keberadaan ponsel pintar dan pandemi COVID-19. Menurut Pusat Nasional untuk Anak Hilang dan Tereksploitasi, laporan bulanan mengenai materi semacam itu meningkat dua kali lipat dari sekitar 1 juta pada bulan Maret 2019 menjadi 2 juta pada tahun kemudian. Laporan meningkat sebesar 35% tambahan dari tahun 2020 hingga 2021." Problematika diatas adalah salah satu contoh dimana Kejahatan Mayantara dilakukan secara global, dimana penyebaran dilakukan melewati website-website illegal yang dibuat untuk mencari keuntungan semata. Mobilitas kejahatan yang tinggi tidak hanya terjadi di dalam satu wilayah, tetapi juga antar wilayah, bahkan lintas wilayah dan lintas batas negara [8].

Bentuk-bentuk *Cyber Crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 4 (empat) kualifikasi umum, yaitu:

1. Kejahatan Mayantara yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer
    a. *Illegal access* (akses secara tidak sah terhadap sistem komputer)
    b. *Data Interference* (mengganggu data komputer)
    c. *System Interference* (mengganggu sistem komputer)
    d. *Illegal Interception in the Computers, system and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)
    e. *Misuse of devices* (menyalahgunakan peralatan komputer)
2. Kejahatan Mayantara yang berhubungan dengan komputer: pemalsuan dan penipuan (*computer related offences; forgery and fraud).*
3. Kejahatan Mayantara yang bermuatan pornografi anak *(content-related offences, child phornography)*
4. Kejahatan Mayantara yang berhubungan dengan hak cipta *(offences-related of infringements of copyright)* [9]

Berdasarkan berbagai bentuk Kejahatan Siber yang telah disebutkan, dapat disimpulkan bahwa diperlukan adanya hukum yang menetapkan regulasi untuk menanggulangi dan mencegah Kejahatan Siber di kalangan masyarakat Indonesia. Hal ini menjadi mendesak mengingat Indonesia saat ini berada dalam situasi kritis terkait keamanan dunia maya (*cyber-security*), dengan fakta bahwa tingkat kejahatan siber di Indonesia telah mencapai tahap yang sangat memprihatinkan. Salah satu fakta yang menunjukkan bahwa kejahatan siber di Indonesia sudah berada pada tingkat yang mengkhawatirkan adalah data dari CIA, yang mengungkapkan bahwa kerugian akibat tindak kejahatan yang terjadi dengan memanfaatkan dunia maya di Indonesia telah mencapai 1,20% dari total kerugian kejahatan siber secara global [10]. Hasil penelitian dari Lembaga Riset Telematika Sharing Vision menunjukkan bahwa pada tahun 2013, Indonesia menempati peringkat pertama sebagai target utama kejahatan dunia maya. Penelitian tersebut mengungkapkan bahwa sepanjang tahun 2013 terjadi sekitar 42 ribu serangan siber setiap harinya [11]. Pemberantasan kejahatan siber di Indonesia bukanlah tugas yang mudah, mengingat karakteristik unik dari kejahatan tersebut. Terdapat sejumlah kendala dalam upaya penanggulangan kejahatan ini, beberapa di antaranya meliputi:

1. Karakteristik kejahatan siber menunjukkan bahwa jenis kejahatan ini dapat melintasi batas yurisdiksi negara, sementara perjanjian internasional yang mengatur penegakan hukum terhadap kejahatan siber masih sangat terbatas.
2. Kebijakan penal dalam penanggulangan kejahatan siber belum didukung dengan kebijakan non-penal, seperti kebijakan di lingkungan kerja, kebijakan pada aplikasi, kebijakan di sekolah, dan lain sebagainya.
3. Penegak hukum harus menghadapi miliaran netizen (pengguna internet) dengan berbagai macam perilaku di dunia maya. Keterbatasan sumber daya yang dimiliki oleh penegak hukum menjadi salah satu tantangan besar dalam upaya penanggulangan kejahatan siber.
4. Kurangnya barang bukti dalam pengungkapan kasus merupakan tantangan besar. Dalam beberapa kasus di dunia maya, kejahatan terjadi melalui aplikasi atau media

yang dioperasikan di luar negeri, yang menyulitkan pihak kepolisian untuk meminta bukti kepada penyedia layanan yang berada di luar yurisdiksi Indonesia [12].

Poin-poin di atas merupakan tantangan dalam menghadapi kejahatan siber di Indonesia, di mana aparat penegak hukum dan pengaturan regulasi di Indonesia harus terus berkembang dan selaras dengan perkembangan kejahatan siber itu sendiri.

3.2 Kepastian, keadilan, dan kemanfaatan hukum terkait Kejahatan Mayantara di Indonesia melalui hukum pidana.

Tenaga ahli yang terbatas untuk melakukan penyidikan menjadi faktor tingkat keberhasilan pihak kepolisian memberantas kasus kejahatan dunia maya menjadi sangat kecil. Dengan terbatasnya tenaga ahli, hal ini menjadi kendala dalam menyelesaikan kasus kejahatan dunia maya dengan waktu yang efisien, sehingga para pelaku dapat memanfaatkan situasi ini untuk menjalankan aksinya dengan lebih leluasa. Rekonstruksi hukum terhadap kejahatan dunia maya mencakup beberapa dimensi utama. Pertama, peningkatan keamanan teknologi informasi harus menjadi prioritas. Hal ini mencakup penguatan sistem keamanan dunia maya untuk melindungi infrastruktur kritis dan data sensitif. Kedua, literasi mengenai keamanan dunia maya di kalangan masyarakat perlu ditingkatkan agar mereka dapat merespons ancaman digital dengan lebih bijaksana [13].

Hukum pidana di Indonesia saat ini masih bergantung pada hukum khusus, seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian diubah dengan UU No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan selanjutnya diubah lagi dengan UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008. Salah satu contoh pasal yang mengatur tentang kejahatan dunia maya dalam UU No. 11 Tahun 2008 terdapat dalam Bab VII mengenai Perbuatan yang Dilarang, yaitu Pasal 27 Ayat (1) yang berbunyi: "(1) Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan." Pasal ini dilanjutkan dengan Ayat (2) mengenai muatan perjudian, Ayat (3) tentang penghinaan dan/atau pencemaran nama baik, serta Ayat (4) tentang muatan pemerasan dan/atau pengancaman [13].

Pasal 27 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut memformulasikan kriminalisasi beberapa tindakan kejahatan maya di Indonesia, di mana kriminalisasi merujuk pada tindakan atau penetapan oleh penguasa mengenai perbuatan-perbuatan tertentu yang oleh masyarakat atau golongan tertentu dianggap sebagai perbuatan yang dapat dipidana, sehingga menjadi tindak pidana. Tindakan yang melanggar kesusilaan seperti yang tercantum dalam Ayat (1) dapat dikaitkan dengan Pasal 281, 282, 283, dan 283 bis KUHP, sedangkan tindakan pemerasan dan/atau pengancaman yang tercantum dalam Ayat (4) dapat dikaitkan dengan Pasal 368 Ayat (1) KUHP.

Diresmikannya UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang akan berlaku pada tahun 2026 mendatang telah membuka jalan bagi landasan regulasi hukum pidana Indonesia yang sejalan dengan perkembangan zaman. Salah satu contohnya adalah pengaturan dalam Bagian Kelima tentang Tindak Pidana terhadap Informatika dan Elektronika, yang mencakup:

1. Pasal 332 ayat (1) : "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem elektronik milik Orang lain dengan cara apa pun, dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V.
2. Pasal 334 huruf d : Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau dipidana denda paling banyak kategori IV, setiap Orang yang: d. menyebarkan, memperdagangkan, atau memanfaatkan Kode Akses atau Informasi yang serupa dengan hal tersebut yang dapat digunakan untuk menerobos Komputer atau sistem elekronik dengan maksud menyalahgunakan yang akibatnya dapat memengaruhi sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri [14].

Dua pasal dalam UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana dapat menjadi dasar yang kuat untuk menghadapi Kejahatan Mayantara yang sedang marak terjadi. Selain itu, pemerintah Indonesia juga telah mengesahkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Salah satu bentuk perlindungan tersebut diatur dalam Bab VI, yang membahas kewajiban Pengendali dan Prosesor Data Pribadi dalam pengolahan data pribadi. Pasal 19, misalnya, menyebutkan bahwa Pengendali dan Prosesor Data Pribadi mencakup: setiap orang, badan publik, dan organisasi internasional. Pasal 35 dan 36 lebih lanjut menjabarkan kewajiban khusus yang harus dipatuhi oleh pihak-pihak tersebut.

Pasal 35

"Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan:

a. penyusunan dan penerapan Langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang berentangan dengan ketentuan peraturan perundangan-undangan; dan
b. penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi."

Pasal 36

"Dalam melakukan pemrosesan Data Pribadi, Pengendali Data Pribadi wajib menjaga kerahasiaan Data Pribadi." [15]

Kedua pasal tersebut memiliki kaitan langsung dengan berbagai bentuk Kejahatan Mayantara yang saat ini semakin marak di Indonesia. Bertambahnya jumlah data pribadi masyarakat seiring dengan kemajuan teknologi dan semakin mudahnya akses internet di seluruh negeri menjadikan perlindungan data sebagai tanggung jawab yang tidak hanya berada di tangan individu, tetapi juga pemerintah. Potensi terulangnya kasus seperti kasus Bjorka, yang mengancam privasi masyarakat Indonesia, menjadi pengingat akan pentingnya regulasi yang kuat.

Pengesahan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana membuka peluang baru dalam upaya melawan dan menanggulangi Kejahatan Mayantara di Indonesia. Adanya regulasi ini memberikan kerangka hukum yang jelas, sehingga masyarakat dan pihak-pihak terkait dapat memahami batasan-batasan hukum yang berlaku serta mengambil langkah preventif untuk melindungi diri dari ancaman Kejahatan Mayantara.

Regulasi ini bertujuan untuk memberikan kepastian hukum bagi semua pihak yang terlibat. Dengan memahami konsekuensi dari pelanggaran hukum yang telah diatur secara tegas dalam undang-undang, setiap individu maupun entitas diharapkan lebih berhati-hati dalam menggunakan teknologi informasi dan elektronik. Upaya ini membantu menciptakan ekosistem yang lebih tertib dan terkontrol, sehingga dapat mencegah munculnya ketidakpastian yang berpotensi merugikan berbagai pihak.

Dalam kerangka keadilan hukum, sangat penting memastikan bahwa sanksi yang dijatuhkan kepada pelaku kejahatan mayantara sebanding dengan tingkat pelanggaran yang dilakukan. Regulasi yang menetapkan hukuman sesuai dengan tingkat kejahatan menjadi fondasi untuk mewujudkan keadilan hukum. Selain itu, proses hukum yang transparan dan adil berperan penting dalam penegakan keadilan, di mana semua pihak harus mendapatkan akses yang setara terhadap proses hukum tanpa adanya diskriminasi dalam penerapannya.

Dengan hadirnya regulasi yang mengatur Kejahatan Mayantara, seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Indonesia telah mengambil langkah awal yang signifikan untuk menghadapi dan menangani ancaman kejahatan mayantara. Melalui penerapan prinsip kemanfaatan, kepastian, dan keadilan hukum, diharapkan tercipta ekosistem yang lebih aman dan tertib dalam penggunaan teknologi informasi dan elektronik di tanah air.

4. KESIMPULAN

Tantangan dalam menghadapai perkembangan teknologi yang kian maju sangat kompleks terlebih li menghadapi perkembangan hukum pidana dibidang kejahatan mayantara. dikarenakan membutuhkan pendekatan yang kompleks dan membutuhkan pendekatan yang holistik. antara kejahatan komputen dan kejahatan mayantara memiliki hubungan yang erat dan selalu berkembang dengan seiringnya perkembangan teknologi. dalam hal ini tertunya harus banyak yang dipersiapkan salah satunya dengan meningkatkan kerjasama internasional, hal ini dikarenakan menyesuaikan dengan kemajuan teknologi. tentu saja dalam ini terdapat banyaknya tantangan mulai dari harus meningkatkan regulasi penegakan hukum,termasuk yuridiksi lintas mayantara, kurang sumber daya penegak hukum dan harus mengumpulkan bukti elektronik. maka dari itu diperlukan upayah perkembangan terus menerus yakni pada sistem penegakan hukum,pengembangan regulasi yang lebih komprehensif serta kerja sama internasional guma memastikan agar penenkan hukum yang kuat dapat lebih efektif dalam mengurangi kejahatan mayantara yang ada di Indnesia.

Lalu regulasi regulasi hukum pidana terkait kejahatan mayantara diindonesia seperti UU No. 11 Tahun 2009 tentnag informasi transaksi elektronik, UU No. 27 Tahun 2022 tentang perlindungan data pribadi serta UU No. 1 Tahun 2023 tentang KUHP, dapat menjadi fondasi yang penting untuk melawan ancaman dari kejahatan mayantara dengan memberikan kepastian hukum serta memastikan keadilan dalam penegakan hukum, agar dapat menciptakan suasana yang aman dalam penggunaan teknologi elrktronik.

REFERENSI

[1] Supanto. “Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy” 5, No. 1 (2016).

[2] Dewi, Intan Rakhmayanti. "Hacker Bjorka Is Back, Data Apa Saja Yang Pernah Dibocorkan?" Cnbc Indonesia. Last Modified 2022. Https://Www.Cnbcindonesia.Com/Tech/20221111075351-37-386931/Hacker-Bjorka-Is-Back-Data-Apa-Saja-Yang-Pernah-Dibocorkan.
[3] Kim, Chris, Barrie Newberger, And Brian Shack. "Computer Crimes." American Criminal Law Review. Last Modified 2012. Https://Www.Ojp.Gov/Ncjrs/Virtual-Library/Abstracts/Computer-Crimes-7#:~:Text=The U.S. Department Of Justice,%2c Investigation%2c Or Prosecution.%22.
[4] Itu (2015), Understanding Cybercrime: Phenomena, Challenges And Legal Response, Itu, Geneva, Http://Handle.Itu.Int/11.1002/Pub/80c0b5e9-En.
[5] Abdul Wahid Dan Mohammad Labib, 2005, Kejahatan Mayantara (Cyber Crime), Bandung, Refika Aditama.
[6] Windara, I Made Agus, And Aa. Ketut Sukranatha. "Kendala Dalam Penanggulangan Cybercrime Sebagai Suatu Tindak Pidana Khusus." Kertha Negara 1, No. 4 (2013): 1–5.
[7] Huizar, T. (2023). No Title. Usa Today. Https://Www.Usatoday.Com/Story/Opinion/2023/03/10/How-Social-Media-Emboldens-Abusers/11413209002/
[8] Liviani, Miftakhur Rokhman Habibi-Isnatul. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia" 23, No. 2 (2020).
[9] Aldriano, Muhammad Anthony, And Mas Agus Priyambodo. "Cyber Crime Dalam Sudut Pandang Hukum Pidana." Jurnal Kewarganegaraan 6, No. 1 (2022): 2.
[10] Hafid, Muhammad, Favian Zhuhri Firjatullah, Billyco Windy Pamungkaz, Studi Magister, Ilmu Hukum, Universitas Wijaya, And Kusuma Surabaya. "Tantangan Menghadapi Kejahatan Cyber Dalam Kehidupan Bermasyarakat Dan Bernegara." Pendidikan Tambusai 7, No. 2 (2023): 9548–9556.
[11] Anwar, Muh. Chaerul, Muh. Arfhani Ichsan, And Fadli Yaser Arafat. "Perspektif Hukum Pidana Dalam Kejahatan Cyber Crime." Jurnal Hukum Universitas Sulawesi Barat 6 (2023): 1–17.
[12] Bunga, Dewi. "Politik Hukum Pidana Terhadap Penanggulangan Cybercrime." Jurnal Legislasi Indonesia 16, No. 1 (2019): 1–15. Https://Www.Cybersecurityintelligence.Com/Blog/Fbis-Cybercrime-.
[13] Uu No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elekronik, Pasal 27
[14] Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, Pasal 332 Ayat (1) Dan 334 Huruf D.
[15] Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Pasal 19, 35 Dan 36.