

Perlindungan Data Pribadi di Basis Data InternasionaI Terhadap *Cyber Crime* menurut Perspektif Undang-Undang Indonesia

Bagus Zaidan Cahyo Prabowo¹, Arista Candra Irawati², Hani Irhamdessetya³, Indra Yuliawan⁴

^{1,2,3,4}Univeritas Ngdui Waluyo

E-mail: baguszaidan16@gmail.com¹, acitujuhsatu@gmail.com², haniirhamdessetya@unw.ac.id³, indrayuliawan@unw.ac.id⁴

Article History:

Received: 11 Juni 2025

Revised: 25 Juni 2025

Accepted: 27 Juni 2025

Kata Kunci: *Data Pribadi, Kejahatan Siber, Internasional*

Abstrak: *Era digital saat ini membawa berbagai kelebihan dan kekurangan, terutama dalam akses informasi dan pengelolaan data pribadi. Meskipun kemajuan teknologi, seperti cloud computing, memudahkan akses informasi, risiko penyalahgunaan data pribadi semakin meningkat, terutama dalam sektor perdagangan, perbankan, pendidikan, dan pemerintahan. Konsep digital dossier mengumpulkan informasi pribadi yang berpotensi disalahgunakan, menimbulkan tantangan dalam perlindungan data. Kejahatan siber, seperti pencurian identitas dan ransomware, menjadi ancaman serius yang memerlukan perhatian lebih. Di Indonesia, meskipun telah ada ketentuan hukum yang berkaitan dengan keamanan data individu, penegakan hukum dan kesadaran masyarakat masih menjadi kendala. Oleh sebab itu, sinergi antara pemerintah, bidang usaha swasta, dan komunitas adalah kunci untuk menciptakan suasana yang aman bagi data pribadi. Kerjasama internasional juga diperlukan untuk menghadapi kejahatan siber yang semakin kompleks. Upaya bersama dalam meningkatkan kesadaran dan regulasi akan memastikan perlindungan data pribadi, menjaga hak individu di tengah kemajuan teknologi yang pesat.*

PENDAHULUAN

Era Digital saat ini, memiliki kelebihan dan kekurangan yang bermacam macam. Salah satu dari kelebihan tersebut adalah mudahnya akses informasi dampak dari perkembangan teknologi yang pesat. Namun, disamping kelebihan dalam mudahnya akses informasi terdapat kelemahan yang dianggap sangat fatal terlebih lagi pada informasi yang berkaitan dengan data pribadi seseorang. Dengan demikian dianggap sangat fatal disebabkan berbagai bidang hidup menggunakan informasi pribadi seperti halnya bidang perdagangan, (*e-commerce*), media sosial, bidang keuangan atau perbankan, bidang pendidikan (*online education*), bahkan bidang pemerintahan (*e-government*). Ruang lingkup informasi pribadi dapat meliputi penyimpanan, riwayat, dan akses mengenai bidang bidang yang sudah di sebutkan sebelumnya. Perkembangan ekonomi saat ini, berefek pada informasi pribadi menjadi sumber daya yang sangat bernilai karena

nilai ekonominya yang menjulang, dengan demikian sering dimanfaatkan oleh sektor perdagangan. Fenomena ini disebut sebagai digital *dossier*, yang merujuk pada akumulasi data mengenai individu dalam jumlah besar melalui teknologi digital, dimulai sejak awal tahun 1970-an dengan komputer dan terus berkembang hingga saat ini dengan internet.

Salah satu contoh dampak dalam transformasi teknologi diatas melahirkan sebuah teknologi yang kemudian di beri nama *Cloud Computing* yang didapat dari penggabungan teknologi dan internet. *Cloud Computing* memungkinkan seseorang untuk mengakses dimanapun dan kapanpun mengenai informasi pribadi dengan menggunakan internet. Kelebihan dari revolusi teknologi ini antara lain mudah untuk mengakses informasi pribadi di berbagai tempat atau *platform* selagi mempunyai internet. Setiap aktivitas yang telah disebutkan sebelumnya diperlukannya validasi identitas oleh pengelola pemrosesan data. Proses ini bertujuan untuk memastikan bahwa pelaku aktivitas elektronik adalah manusia, bukan bot, dan dapat dimintai pertanggungjawaban secara hukum. Oleh karena itu, pengelola layanan mewajibkan setiap penerapan untuk memberikan informasi individu, seperti nama, domisili beserta tanggal lahir, alamat, nomor KK, NIK, status perkawinan, serta identitas lainnya, yang merupakan bagian dari data pribadi.

Konsep informasi data pribadi yang menggunakan *Cloud Computing*, juga memiliki arti bahwasannya informasi tentang data pribadi dapat disimpan dan dikelola di luar negeri atau diluar domisili dari pemilik informasi data pribadi tersebut. Dalam perundang-undangan yang ada di Indonesia, penyimpanan dan pengelolaan data informasi pribadi pada luar negeri sendiri diperkuat oleh PP (Peraturan Pemerintah) No. 71 Tahun 2019 mengenai Sistem Penyelenggaraan dan Transaksi Elektronik (PTSE) dalam Pasal 21 Ayat (1) menyatakan bahwa: “*Penyelenggara Sistem Elektronik Lingkup Privat dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di wilayah Indonesia dan/atau di luar wilayah Indonesia*”. Dijelaskan Pasal 1 dari PP Nomor 71 Tahun 2019 menyatakan yang dimaksud dengan penyelenggara sistem elektronik dalam lingkup privasi mencakup pelaksanaan Sistem berbasis Elektronik oleh individu, perusahaan, dan lingkup masyarakat umum. Dari pernyataan kedua klausul diatas dapat diketahui bahwasannya penyimpanan informasi data pribadi dilegalkan untuk dilaksanakan di kawasan Indonesia atau luar negeri melalui penyelenggaranya meliputi orang perorangan, badan usaha, atau masyarakat Indonesia yang memiliki kepentingan. Namun hal tersebut menimbulkan kontra terhadap perspektif hukum. Ketua Asosiasi Cloud Computing (Alex Budiyo) juga menyampaikan bahwasannya, Ketentuan ini memicu negara tidak dapat melindungi data rakyatnya (Rakhmayanti, 2019). Jelas permasalahan tersebut mengkhawatirkan tidak hanya bagi masyarakat, namun juga bagi pemerintah yang bertanggung jawab dalam melindungi data pribadi milik rakyatnya.

Perlindungan Data menjadi fokus utama setelah mengetahui permasalahan diatas. Kejahatan siber atau yang sering disebut Kejahatan Mayantara, *Cyber Crime* atau *Cyber Security* sedang marak terjadi. Keamanan atau kejahatan siber merujuk pada jenis kejahatan yang memanfaatkan ruang siber dan kemajuan dalam Teknologi Informasi dan Komunikasi untuk melaksanakan aksinya. Tindak kejahatan yang bersifat transnasional memerlukan pendekatan khusus yang terpadu demi kebaikan hubungan antar negara sebagai perwujudan dari penanganan kasus kejahatan siber. Usaha untuk mencapai keselarasan menjadi tantangan besar bagi negara, mengingat setiap negara memiliki perspektif yang berbeda dalam menangani kasus kejahatan siber. Selain kerjasama antar negara, UU Nomor 19 Tahun 2016 yang merupakan amandemen dari UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga memiliki peran penting dalam pelaksanaan perlindungan data pribadi. Perlindungan data pribadi di Indonesia masih lemah karena negara ini belum memiliki lembaga yang mengawasi perlindungan data pribadi. Dengan

demikian, Undang-Undang Nomor 19 Tahun 2016 yang merupakan amandemen dari UU Informasi dan Transaksi Elektronik menjadi perisai perlindungan informasi data pribadi.

METODE PENELITIAN

Metode Penelitian pada artikel menggunakan penelitian kualitatif. Menurut salah satu ahli, Penelitian kualitatif adalah jenis penelitian yang bertujuan untuk mencari informasi secara mendalam dan terbuka mengenai berbagai tanggapan. Metode ini mendorong individu untuk mengungkapkan pemikiran mereka tentang suatu topik tanpa memberikan banyak pedoman atau arahan. Maka studi ini berfokus kepada deskriptif analisis, penelitian atas kejadian yang berhubungan dengan kondisi saat ini.

Teknik pengumpulan data dalam metode penelitian menggunakan pendekatan studi pustaka. Peneliti mengumpulkan referensi seperti majalah, buku, dan artikel terdahulu yang relevan dengan masalah dan tujuan penelitian. Sumber-sumber tersebut dianggap sebagai data yang akan diolah dan dianalisis, mirip dengan implementasi para ahli sejarah, sastra, dan bahasa. Terdapat berbagai pandangan lain terkait studi pustaka. Pendapat tersebut disampaikan oleh Sarwono, beliau menjelaskan pengertian studi pustaka merupakan kegiatan mempelajari berbagai buku referensi serta hasil penelitian sebelumnya yang sejenis yang berguna untuk mendapatkan landasan teori mengenai masalah yang akan diteliti (Azis, 2023). Dari dua pendapat diatas dapat diketahui penelitian dengan Teknik pengumpulan data studi pustaka tidak hanya meneliti dari sumber buku saja, namun juga dapat memilih sumber dari penelitian sebelumnya berupa artikel, jurnal, dan pernyataan asalkan sejenis dan muatan dalam penulisan masih memiliki hubungan terkait dengan isu yang akan diteliti.

HASIL DAN PEMBAHASAN

Teknologi Informasi Data Pribadi Di Luar Negeri dalam Bindang Kehidupan Masyarakat

Setiap bidang kehidupan masyarakat kini sudah memanfaatkan informasi data pribadi dengan mudah sebagai salah satu aspek kemajuan teknologi. Lima (5) Bidang penting dari kehidupan bermasyarakat umum yang akan dibahas mulai dari perdagangan atau bisnis, perbankan atau keuangan, sosial masyarakat, pendidikan, bahkan pemerintahan. Sebelum memasuki ruang lingkup dampak dari kemajuan teknologi informasi data pribadi perlu diketahui terlebih dahulu lebih dalam mengenai teknologi informasi data pribadi.

Teknologi Informasi ialah teknologi yang digunakan untuk pengolahan data dengan beragam cara sebagai tujuan mencapai informasi yang memiliki kualitas. Informasi ini harus relevan, akurat, dan tepat waktu, serta digunakan untuk keperluan pribadi, bisnis, dan pemerintahan, menjadi strategis dalam pengambilan keputusan. Sebab peran teknologi informasi, dapat mengetahui data pribadi yang mengacu kepada kehidupan sehari-hari mulai dari kesehatan, profesi, perdagangan, dan kerja sama antar individu, bahkan hobi seseorang tanpa mengenal batasan mengenai ras, golongan, negara, ideologi, bahkan strata ekonomi seseorang. Penyimpanan informasi data pribadi dapat dilakukan di dalam maupun luar negeri. Tergantung pada kebijakan perusahaan atau perusahaan dalam menyimpan informasi data pribadi.

Pada kehidupan masa mendatang, sektor teknologi informasi ini bakal mendominasi berbagai bidang di kehidupan individu atau kelompok. Bagi mereka yang dapat menguasai teknologi informasi ini berpeluang besar menjadi pemimpin dalam dunianya. Secara khusus yang dapat dilihat sangat berdampak pada teknologi informasi ini berupa bidang perdagangan atau bisnis, perbankan atau keuangan, sosial masyarakat, pendidikan, dan pemerintahan. Terdapat alasan yang signifikan mengapa bidang-bidang yang disebutkan sebelumnya terdampak teknologi informasi

antara lain:

1. Bidang Perdagangan atau Bisnis

Seiring dengan laju manusia dalam berkembang, metode dan alat yang digunakan untuk perdagangan terus mengalami perubahan. Salah satu tipe perdagangan yang semakin mempermudah adalah *e-commerce*. Dalam konteks ini, *e-commerce* terdiri dari dua kata, di mana "e" merupakan singkatan dari *electronic* dan "*commerce*" berarti perdagangan. Jaringan publik dimanfaatkan sebagai proses bertransaksi, dan perbuatan jual beli tanpa harus bertemu langsung dengan penjual atau pembeli. Kegiatan perdagangan ini sendiri menghubungkan antara perusahaan individu atau kelompok dengan para konsumen tanpa melibatkan pertemuan langsung. Hal ini secara tidak langsung melibatkan data pribadi sejumlah individu yang melakukan hubungan perdagangan melalui *e-commerce*. Karena sifat dari teknologi informasi yang memberikan informasi mengenai data pribadi kepada penjual begitu juga sebaliknya agar kegiatan jual beli dapat terlaksana. Kejelasan mengenai informasi penjual maupun pembeli, mengakibatkan timbulnya rasa kepercayaan sehingga kegiatan perdagangan dapat berjalan dengan lancar.

2. Bidang Perbankan atau Keuangan

Untuk mendukung keberhasilan operasional lembaga keuangan atau perbankan memerlukan sistem informasi yang cekatan dan mudah diakses oleh nasabah. Hal ini bergantung pada teknologi informasi. Semua transaksi ini dapat dilakukan dengan cepat dan efisien. Hal itu dimaksudkan sebagai bentuk sistem keamanan pada perusahaan yang bergerak pada bidang keuangan. Sebuah perusahaan perbankan atau keuangan tidak akan mempercayai begitu saja tanpa keterangan informasi yang jelas mengenai nasabah yang akan menggunakan jasa dari perusahaan tersebut. Demikian juga dengan nasabah yang tidak bisa asal percaya terhadap perusahaan yang dipercaya untuk menyerahkan urusan keuangannya. Tidak hanya hubungan antara perusahaan dan individu, perilaku hubungan kerja sama dalam bidang keuangan ini juga berpengaruh pada individu dan individu lainnya. Maka dari itu informasi data pribadi akan selalu diberikan sebagai perwujudan kepercayaan dan keabsahan kegiatan keuangan atau perbankan yang dilakukan.

3. Bidang Sosial Masyarakat

Pengaruh kemajuan teknologi informasi ini secara signifikan mengubah pola hidup masyarakat sehari-hari. Perilaku bersosial yang paling sering dilakukan oleh masyarakat dalam memanfaatkan teknologi informasi yakni pertukaran data dengan mudah yang bertujuan menunjang kemudahan dalam pekerjaan masyarakat. Yang disebut dengan pertukaran data secara rinci adalah pertukaran informasi melalui *e-mail* yaitu akronim dari *electronic mail*, sebuah surat elektronik yang dikirim menggunakan sarana media elektronik seperti komputer atau *smartphone*. Selain pertukaran informasi, sudah banyak yang mengetahui mengenai media sosial berbasis elektronik. Media sosial berbasis elektronik ini dapat menghubungkan orang perorangan atau kelompok dengan individu atau kelompok lain tanpa dilakukannya pertemuan langsung. Sebagai bentuk aplikasi dari hubungan tersebut diperlukannya sarana yang juga dalam pengoperasian sarana tersebut membutuhkan informasi data pribadi sebagai upaya mempermudah individu mengenali satu sama lain di dalam sarana tersebut.

4. Bidang Pendidikan

Kecenderungan Pendidikan di masa kini telah bergeser dari Pendidikan tatap muka menjadi Pendidikan yang lebih terbuka. Pendapat ini juga di kemukakan oleh ahli (Mason, 2000) secara singkat bahwasannya Pendidikan akan lebih mengarah ke jaringan informasi sebagai bentuk interaksi dan memungkinkan untuk kegiatan pembelajaran tidak berada pada gedung sekolah. Tidak hanya kegiatan pembelajaran saja, sumber bahan untuk kegiatan pembelajaran seperti halnya pustaka atau perpustakaan akan beralih menjadi informasi yang mudah dijangkau tanpa harus susah

payah mencarinya di rak buku akibat dari perkembangan teknologi informasi yang pesat. Susah dihindari jika informasi data pribadi mulai dari pengajar hingga murid tidak masuk dalam sistem jaringan informasi.

5. Bidang Pemerintahan

Pemerintahan dituntut untuk selalu memberi pelayanan kepada masyarakat seiring perkembangan zaman dan teknologi dengan baik dan terpadu. Jelas pemerintahan tidak tinggal diam dalam menyikapi tuntutan tersebut. Tentu hal ini tidak lepas dari pemanfaatan teknologi untuk mengimbangi perkembangan zaman yang beriringan dengan pesatnya perkembangan teknologi. Dalam penerapannya, pemerintah memfasilitasi rakyatnya dengan menyediakan *e-government*. *E-Government* adalah hasil dari kinerja pemerintahan dengan maksud agar pemerintahan dapat dengan mudah dan praktis dalam berinteraksi dengan masyarakat. Dalam penerapannya menimbulkan kontra sebab dimasukkannya unsur pemerintahan dalam teknologi informasi ini memberi resiko yang tinggi. Apalagi pemerintahan adalah pemegang urusan dalam negara yang apabila salah dalam penerapannya, informasi data pribadi mengenai pejabat pemerintahan dan rakyat yang berurusan dengan pemerintahan masuk ke dalam jaringan informasi yang notabene Sangat mudah untuk diintervensi berbagai elemen luar yang tidak bertanggung jawab. Disamping itu, maksud dari pemanfaatan teknologi informasi juga memiliki peranan penting. Tetap saja, hal tersebut melibatkan informasi data pribadi pejabat pemerintahan maupun masyarakat umum.

Salah satu contoh metode penyimpanan data pribadi dengan pusat data di luar negeri dan marak digunakan yaitu *cloud computing*. *Cloud Computing* ialah kompilasi atas beberapa sumber daya yang terintegrasi dan dipergunakan melalui web. *Cloud Computing* berdasar pada *grid computing* yang memiliki aksud menciptakan skalabilitas suatu sistem menjadi sangat besar dengan cara menyatukan berbagai sumber daya komputer menjadi satu sumber. Sehingga seringkali *cloud computing* disebut sebagai *grid computing* yang tergabung dengan virtualisasi.

Penggunaan *cloud computing* paling sering digunakan oleh masyarakat terutama dalam bidang perdagangan. Tanpa memerlukan infrastruktur, cukup dengan perusahaan menyediakan fasilitas penyimpanan di internet sebagai dampak dari perusahaan yang memberi kan jasa penyimpanan sumber daya yang menggunakan *cloud computing*. Selain itu, biaya yang dikeluarkan bersifat ekonomis karena adanya penekanan Biaya infrastruktur dan perangkat lunak sebab telah didukung oleh perusahaan yang menawarkan layanan cloud computing.

Cyber Crime Sebagai Ancaman Data Pribadi

Beberapa dekade berlalu, teknologi informasi berkembang pesat, disamping itu, konsekuensi dari perlembangan tersebut juga besar salah satunya adalah *Cyber Crime*. Dapat disimpulkan dalam buku Pengantar Siber karya (Edrissy, 2019) *Cyber Crime* atau dapat disebut Kejahatan Siber dan Kejahatan Mayantara merupakan kegiatan kriminal di ranah digital yang memanfaatkan komputer sebagai alat dan internet sebagai penunjang.

Salah satu jasa data yang mayoritas pusat datanya berbasis di luar negeri adalah penggunaan layanan cloud computing mengandung risiko yang mungkin terjadi., terutama terkait eksploitasi data privasi konsumen, termasuk informasi operasi usaha bersifat rahasia dengan intervensi dari instansi pemerintah atau penyedia layanan berbasis cloud. Sering penyedia layanan cloud memiliki pusat data yang berlokasi di luar batas negara atau di luar yurisdiksi nasional. Hal ini membuat penyelesaian masalah penyalahgunaan pengelolaan data privasi pelanggan menjadi sulit, karena melibatkan perbedaan yurisdiksi dan peraturan terkait data privasi antar negara. Selain itu di AS (Amerika Serikat), perusahaan swasta memiliki kebebasan yang diberikan oleh pemerintah untuk mengatur operasional mereka mereka sendiri dalam manajemen data yang bersifat *self-*

regulatory.

Bentuk kejahatan siber yang mengkhususkan berhubungan dengan data pribadi ialah *Infringements of privacy* adalah kejahatan informasi data individu seseorang adalah tindakan yang mengkhawatirkan dan bersifat rahasia. Tindakan jahat ini berfokus pada data pribadi yang tersimpan dalam formulir yang dikelola secara komputer, dan apabila data tersebut berada di tangan yang tidak tepat, dapat menyebabkan kerugian bagi korban, baik secara finansial maupun non-finansial, termasuk nomor kartu kredit, kode pin ATM, dan info kesehatan yang bersifat rahasia.

Kesadaran masyarakat akan *Infringements of Privacy* masih sangat minim. Maka dari itu, dapat digolongkan beberapa jenis kejahatan siber yang termasuk dalam bentuk kejahatan *Infringements of Privacy* agar mempermudah kepaahaman masyarakat. Ada beberapa jenis pada kejahatan siber, yaitu: (Ali, 2024)

1. *Phishing*, atau penipuan

Salah satu tindak kejahatan dalam dunia virtual yang paling umum terjadi. Tindakan *phishing* melibatkan penggunaan e-mail atau pesan palsu yang dirancang untuk menipu korban agar memberikan data informasi, baik yang bersifat individu maupun perusahaan. Dalam kejahatan internet ini, sering kali digunakan teknik rekayasa sosial untuk mendorong korban memberikan informasi rahasia, seperti nomor kartu kredit, nomor rekening, kredensial login, serta data pribadi dan keuangan lainnya. Jenis penipuan ini biasanya melibatkan perangkat lunak berbahaya, seperti worm, trojan, dan virus. Selain itu, penipuan ini sering kali memanfaatkan identitas perusahaan untuk menipu dan merusak kepercayaan pelanggan terhadap merek tertentu, yang pada gilirannya dapat merusak reputasi merek tersebut.

2. Penggelapan atau *identity stealing*,

Ini adalah bentuk pencurian data identitas pribadi, seperti data transaksi yang tidak valid atau tidak sah, yang dapat memicu terjadinya penipuan lainnya. Kejahatan di dunia maya ini melibatkan pencurian informasi pribadi yang digunakan untuk melakukan transaksi ilegal dan aktivitas penipuan atau pencurian lainnya. Akibat dari pencurian data identitas pribadi, beberapa dampak yang mungkin terjadi meliputi:

- a. Tagihan kredit yang tidak jelas
- b. Penarikan dana dari rekening bank yang tidak diketahui.
- c. Kerugian finansial
- d. Gangguan psikologis
- e. *Problem* hukum

3. *Offensif Ransomware*,

Ini adalah serangan terhadap jaringan komputer yang bertujuan untuk pemblokiran akses arsip korban, sehingga aksesnya diblokir hingga tebusan dibayarkan. Kejahatan jenis ini merupakan pelanggaran terhadap data, di mana korban biasanya diharuskan membayar tebusan untuk mendapatkan kembali akses ke data mereka. Menurut laporan penelitian, 43% organisasi di seluruh dunia yang pernah mengalami serangan ransomware juga telah menghadapi situasi serupa, di mana data mereka terkunci atau terpaksa membayar tebusan untuk data yang telah diretas

Data pribadi harus dilindungi dan kerahasiaannya dijaga agar hak dalam hukum warga negara dapat terjamin. Data pribadi mencakup informasi yang berkaitan dengan identitas individu, seperti Kartu Keluarga Nomor Induk Kependudukan, dan lain-lain. Namun, sangat disayangkan bahwa belakangan ini, dugaan kasus kebocoran data pribadi semakin pesat, bahkan Indonesia menjajaki podium ketiga di dunia dalam hal jumlah kasus kebocoran data terbanyak.

Kejahatan Siber juga tentunya berbeda dengan kejahatan konvensional lainnya. Maka,

beberapa hal yang perlu diketahui masyarakat terhadap tindak kejahatan siber adalah karakter yang khas dibandingkan kejahatan konvensional, antara lain: (Stiawan, 2005)

- a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya
- b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet
- c. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional
- d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. Perbuatan tersebut seringkali dilakukan secara transnasional/ melintasi batas Negara.

Pengaturan Perlindungan Data Pribadi Menurut Hukum Nasional Indonesia

Paradigma hukum baru yang dinamakan hukum siber memanfaatkan teknologi informasi sebagai alat. Istilah ini, yang juga dikenal sebagai Hukum Teknologi Informasi atau Hukum Dunia Maya, menggambarkan kompleksitas interaksi yang ada dunia virtual. Dibalik munculnya hukum baru tersebut, Indonesia masih abu-abu terhadap integrasi peraturan, ketidakjelasan definisi, rendahnya kesadaran masyarakat akan resiko, perlunya pembaruan regulasi yang lebih responsif, serta kolaborasi antar sektor di ranah nasional dan luar negeri. Ada beberapa hukum positif yang berkesinambungan dengan tindak kejahatan siber antara lain:

1. UU No. 1 Tahun 2024 yang merupakan amandemen kedua dari UU Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Dalam pengertian undang-undang tersebut, internet dan semua fasilitasnya dianggap sebagai sarana telekomunikasi
 - a. Pasal 27 B Ayat (1) dalam hal ini, setiap orang yang melakukan penyadapan dan intersepsi untuk mendapatkan informasi pribadi milik orang lain dengan tujuan menguntungkan diri sendiri atau orang lain.
 - b. Pasal 30 dalam Ayat 1,2,3 menegaskan bahwa setiap orang yang mengakses komputer atau sistem elektronik untuk mendapatkan informasi orang lain secara ilegal dalam arti secara paksa dengan cara apapun.
 - c. Pasal 36 segala perbuatan yang ada pada Pasal 30 mengakibatkan kerugian materiil orang lain.
2. UU Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi
 - a. Pasal 65 Ayat (1), (2), (3) dimana pada pasal tersebut memuat larangan mengenai Mengumpulkan, mengungkapkan, dan memanfaatkan data pribadi yang bukan miliknya dengan tujuan untuk mendapatkan keuntungan pribadi oleh pelaku kejahatan siber.
 - b. Pasal 67 memuat sanksi terhadap Pasal 65 Ayat (1), (2), (3)
3. UU Nomor 39 Tahun 1999 mengenai Hak Asasi Manusia
 - a. Pasal 21 dalam penjelasannya keutuhan pribadi rohani dan jasmani menyangkut data pribadi yang tidak boleh digunakan tanpa persetujuan dari pihak yang memiliki data pribadi tersebut
 - b. Pasal 32 menyebutkan kemerdekaan dalam komunikasi yang dilakukan melalui sarana elektronik tidak boleh terganggu, kecuali jika terdapat ketentuan yang mengatur hal tersebut.
4. UU Nomor 10 Tahun 1998 mengenai Perbankan,
 - a. Pasal 40 dalam pasal tersebut dijelaskan bahwasannya kerahasiaan mengenai nasabah adalah tanggung jawab dari Bank. Kerahasiaan tersebut jika di Analisa memuat mulai dari data pribadi hingga transaksi yang dilakukan oleh nasabah kecuali ada ketentuan lain yang

- memperbolehkan diberitahukannya informasi mengenai hal tersebut.
- b. UU Nomor 24 Tahun 2013 mengenai Administrasi Kependudukan
 - c. Pasal 79 Ayat (1), (2), (3), negara menjamin dan berkewajiban menyimpan kerahasiaan dari data pribadi dan di Ayat (4) memuat mengenai ketentuan dalam akses pada data pribadi tersebut yang akan dijelaskan pada peraturan Menteri
 - d. Permenkominfo Republik Indonesia Nomor 20 Tahun 2016 mengenai Perlindungan Data Pribadi dalam Sistem Elektronik. Pada Peraturan Menteri ini, dalam pasal pasalnya menjelaskan mengenai cakupan dalam perlindungan data pribadi termasuk asas perlindungan data pribadi, pernyataan mengenai privasi data pribadi, keabsahan data pribadi, dan persetujuan mengenai kebenaran, status kerahasiaan dan tujuan pengolahan data pribadi. Juga dijelaskan mengenai prosedur perolehan data pribadi dan pengumpulan data pribadi serta hak dan kewajiban pemilik dan penyelenggara sistem informasi data pribadi. Sanksi dan pengawasan dalam data pribadi juga dijelaskan pada Peraturan Menteri tersebut.

Perspektif Hukum Indonesia Terhadap Perlindungan Data Pribadi Di Luar Negeri

Sehubungan dengan NKRI sebagai negara hukum, Pasal 1 ayat (3) UUD 1945 menegaskan bahwa "Indonesia adalah negara hukum." Pernyataan ini mencerminkan pengakuan baik secara yuridis maupun faktual terhadap prinsip supremasi hukum, di mana setiap permasalahan terselesaikan berdasarkan hukum sebagai pedoman tertinggi. Dalam konteks supremasi hukum, pemimpin tertinggi negara bukanlah individu, melainkan konstitusi yang mencerminkan hukum tertinggi. Termuat dalam Pasal 28 G ayat (1) Undang-Undang Dasar NRI Tahun 1945, "setiap individu berhak atas perlindungan diri, keluarga, kehormatan, martabat, dan harta benda yang berada dalam kekuasaannya, serta berhak merasakan keamanan dan perlindungan dari ancaman yang dapat menimbulkan ketakutan untuk melakukan atau tidak melakukan sesuatu yang merupakan hak asasi". Dari kedua klausul dan peraturan perundang-undangan tersebut, jelas bahwa Negara Kesatuan Republik Indonesia sangat memperhatikan perlindungan hukum terhadap data pribadi yang dimiliki masyarakat.

Munculnya kejahatan baru berupa *cybercrime* atau Kejahatan Siber mulai membuat masyarakat dari segala kalangan resah. Pasalnya, kejahatan siber tidak memandang latar belakang dan teritorial masyarakat. Oleh karena itu, perlu adanya penanggulangan secara cepat mengenai kejahatan tersebut. Dalam ruang lingkup peraturan perundang-undangan yang berlaku di Indonesia, secara khusus dan tersendiri dalam penanggulangan kejahatan siber belum ada yang mengaturnya. Karena belum banyak peraturan yang terintegrasi secara keseluruhan, hukum siber termuat secara umum dalam beberapa undang-undang positif di Indonesia. Mengacu pada Pasal 2 dan 5 mengenai Kitab Undang-Undang Hukum Pidana, dijelaskan mengenai prinsip dasar teritorial pemberlakuan hukum pidana dengan adanya dua pembagian berbeda mengacu pada ketentuan berlaku dan diberlakukannya undang-undang tersebut dapat disimpulkan bahwasannya dua pembagian tersebut adalah hukum yang diberlakukan pada ruang lingkup wilayah Indonesia dan diluar ruang lingkup wilayah Indonesia.

Penerapan sebagai instrumen penindak kejahatan siber, hukum internasional tidak lepas dari pembahasan. Sebab hukum internasional berperan sebagai regulasi yang mengatur hubungan antar negara agar interaksi setiap negara dapat berlangsung dengan harmonis dan semestinya tanpa mengesampingkan aspek aspek penting dari masing masing negara demi keadilan hukum. Sementara itu, berhubungan dengan yang sudah disebutkan diatas, dalam Pasal 9 Kitab Undang-undang Hukum Pidana dijelaskan bahwasannya ruang lingkup hukum pidana dalam hal teritorial wilayah pemberlakuannya dibatasi dengan pengecualian yang diakui oleh hukum internasional.

Hal ini dapat dikaitkan dengan Hukum Internasional dalam penerapan sanksi untuk aksi kejahatan siber. Selain instrumen yang dijelaskan diatas, efektifitas kerja sama internasional juga menjadi instrumen penting dalam penanggulangan kejahatan siber dengan prosedur analisis kerjasama antara Interpol dan Europol. Serta kemampuan negara-negara dalam menyediakan informasi, keahlian, dan perhatian terhadap problematika kejahatan siber. Proses ekstradisi dan perjanjian bantuan hukum antar negara bertujuan untuk menuntut pelaku kejahatan siber dan dapat diterapkan di negara yang memiliki yurisdiksi

Beberapa instrumen diatas harus mempunyai kesinambungan yang erat, jika berbicara perlindungan atas informasi data pribadi yang berada di luar negeri. Sebelum menginjak pada perlindungan data pribadi pada server luar negeri, perlu diketahui identifikasi atas prinsip hukum internasional dalam penegakan kejahatan siber. Dalam prinsip kedaulatan dan non intervensi yang prinsip ini dimaksudkan bahwasannya negara memiliki hak untuk mengatur dan menegakkan hukum didalam batas yurisdiksi nya sendiri akan tetapi prinsip ini tidak melupakan aspek hubungan diplomatis antar negara lalu peran kerangka hukum internasional, seperti halnya konvensi Budapest yang memuat panduan komprehensif tentang fasilitas kerja sama internasional mengenai kejahatan siber dan penetapan mekanisme kerja sama lintas negara tetapi tidak pula melupakan tantangan dalam penegakan hukum siber dalam kesenjangan kapasitas negara dalam menangani kejahatan siber dikarenakan negara berkembang sering ketinggalan dalam hal teknologi dan sumber daya yang diikuti dengan perbedaan hukum dan regulasi antar negara dan kepentingan nasional yang berbeda yang dapat menghambat Upayan kerja sama internasional. Disamping tantangan, juga ada peluang dalam kerja sama internasional yang mendesak negara harus mengembangkan kapasitas teknologi dan sumber daya serta pengharmonisasian hukum, dan pembentukan mekanisme dan strategi baru dalam menanggulangi kejahatan siber.

Berkaitan dengan penjelasan mengenai basis data yang bertempat di luar negeri Mengenai penanganan pelaku kejahatan siber apabila pelaku melakukan tindak kejahatan tersebut dan menyangkut keamanan data pribadi masyarakat, tidak mungkin pemerintah Indonesia tutup mata dalam menyikapi kasus tersebut. Maka kebijakan negara Indonesia pada kejahatan siber atas data pribadi yang kejahatannya dilakukan oleh pelaku di luar wilayah Indonesia termaklud Undang-Undang Nomor 1 Tahun 1979 mengenai Ekstradisi dimana pelaku dapat dihakimi di wilayah Indonesia diperkuat dengan Pasal 1 dan 2 dimana orang sekaligus yang dipidana karena disangka melakukan “pembantuan, percobaan, dan pemufakatan jahat” dalam tindak kejahatan yang berasal dari negara asing yang diekstradisi oleh pejabat berwenang untuk menjalani hukuman pidana atau menjalani perintah penahanan menurut hukum Negara Republik Indonesia. Pada Pasal 4 UU Ekstradisi secara singkat daftar kejahatan yang dimaksud terlampir selaku bagan yang tak terputus dari Undang-Undang Nomor 1 Tahun 1979. Rincian detail mengenai daftar kejahatan terletak pada lampiran Undang-Undang No. 1 Tahun 1979, diatur mengenai berbagai tindak kejahatan, antara lain:

1. Pembunuhan.
2. Pembunuhan yang direncanakan.
3. Penganiayaan yang berakibat luka-luka berat atau matinya orang, penganiayaan yang direncanakan dan penganiayaan berat.
4. Perkosaan, perbuatan cabul dengan kekerasan.
5. Persetubuhan dengan seorang wanita di luar perkawinan atau perbuatan-perbuatan cabul dengan seseorang padahal diketahui, bahwa orang itu pingsan atau tak berdaya atau orang itu belum berumur 15 tahun atau belum mampu dikawin.
6. Perbuatan cabul yang dilakukan oleh orang yang cukup umur dengan orang lain sama kelamin

yang belum cukup umur.

7. Memberikan atau mempergunakan obat-obat dan atau alat-alat dengan maksud menyebabkan gugur atau mati kandungan seorang wanita.
8. Melarikan wanita dengan kekerasan, ancaman kekerasan atau tipu muslihat, dengan sengaja melarikan seseorang yang belum cukup umur.
9. Perdagangan wanita dan perdagangan anak laki-laki yang belum cukup umur.
10. Penculikan dan penahanan melawan hukum.
11. Perbudakan.
12. Pemerasan dan pengancaman.
13. Meniru atau memalsukan mata uang atau uang kertas negeri atau uang kertas bank atau mengedarkan mata uang kertas negeri atau kertas bank yang ditiru atau dipalsukan.
14. Menyimpan atau memasukkan uang ke Indonesia yang telah ditiru atau dipalsukan.
15. Pemalsuan dan kejahatan yang bersangkutan dengan pemalsuan.
16. Sumpah palsu.
17. Penipuan.
18. Tindak pidana-tindak pidana berhubungan dengan kebangkrutan.
19. Penggelapan.
20. Pencurian, perampokan.
21. Pembakaran dengan sengaja.
22. Pengrusakan barang atau bangunan dengan sengaja.
23. Penyelundupan.
24. Setiap tindak kesengajaan yang dilakukan dengan maksud membahayakan keselamatan kereta api, kapal laut atau kapal terbang dengan penumpang penumpangnya.
25. Menenggelamkan atau merusak kapal di tengah laut.
26. Penganiayaan di atas kapal di tengah laut dengan maksud menghilangkan nyawa atau menyebabkan luka berat.
27. Pemberontakan atau permufakatan untuk memberontak oleh 2 (dua) orang atau lebih di atas kapal di tengah laut menentang kuasa nakhoda, penghasutan untuk memberontak
28. Pembajakan laut.
29. Pembajakan udara, kejahatan penerbangan dan kejahatan terhadap sarana/prasarana penerbangan.
30. Tindak Pidana Korupsi.
31. Tindak Pidana Narkotika dan obat-obat berbahaya lainnya.
32. Perbuatan-perbuatan yang melanggar Undang-undang Senjata Api, bahan-bahan peledak dan bahan-bahan yang menimbulkan kebakaran.

Termuat pada Pasal 19 Undang-undang No. 1 Tahun 1979 dijelaskan bahwasannya orang yang dimintakan ekstradisi, memiliki ketentuan yang berdasarkan Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana pada Pasal 13 dan 14 huruf J menyatakan bahwa penuntut umum adalah jaksa yang diberi kewenangan untuk melaksanakan ketetapan tersebut, dan penuntut umum wajib menerima salinan hasil ekstradisi dari hakim. Acuan daripada pelaksanaan hukum acara pidana dalam menentukan pelaku dinyatakan bersalah dalam ketentuang undang-undang di Indonesia dijelaskan pada KUHP pada Pasal dijelaskan pada pasal 4 hingga 5 yang berbunyi:

(Pasal 4)

“Ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan di luar Indonesia: 1. Salah satu kejahatan berdasarkan pasal-pasal 104, 106,

107,108,dan 131; 2. suatu kejahatan mengenai mata uang atau uang kertas yang dikeluarkan oleh negara atau bank, ataupun mengenai meterai yang dikeluarkan dan merek yang digunakan oleh Pemerintah Indonesia.; 3. pemalsuan surat hutang atau sertifikat hutang atas tanggungan Indonesia, atas tanggungan suatu daerah atau bagian daerah Indonesia, termasuk pula pemalsuan talon, tanda dividen atau tanda bunga, yang mengikuti surat atau sertifikat itu, dan tanda yang dikeluarkan sebagai pengganti surat tersebut, atau menggunakan surat-surat tersebut di atas, yang palsu atau dipalsukan, seolah-olah asli dan tidak dipalsu”.

(Pasal 5)

“(1) Ketentuan pidana dalam perundang-undangan Indonesia deterspskn bsgi warga negara yang di luar Indonesia melakukan: Salah satu kejahatan tersebut dalam Bab I dan II Buku Kedua dan pasal-pasal 160, 161, 240, 279, 450, dan 451; 2. salah satu perbuatan yang oleh suatu ketentuan pidana dalam perundang-undangan Indonesia dipandang sebagai kejahatan, sedangkan menurut perundang-undangan negara dimana perbuatan dilakukan diancam dengan pidana.”

Hal ini juga diatur dalam Undang-Undang No. 1 Tahun 1979 Pasal 33 ayat (2) berbicara mengenai penetapan surat harus segera di serahkan kepada kementrian huhkum atau yang sekarang disebut Menkum hal ini secara tidak langsung menunda penuntut umum untuk mendapatkan salinan ekstradisi tersebut tetap penuntut umum lah yang memiliki kewenangan pokok untuk melaksanakan ketetapan dalam menguru tindak kejahatan siber.

KESIMPULAN

Di era digital, teknologi informasi telah menjadi bagian yang krusial dalam kehidupan sehari-hari, mempengaruhi berbagai sektor seperti perdagangan, perbankan, sosial, pendidikan, dan pemerintahan. Meskipun kemajuan ini membawa banyak manfaat, seperti kemudahan dalam bertransaksi dan akses informasi, risiko penyalahgunaan data pribadi juga meningkat. Kepercayaan antara individu dan organisasi sangat bergantung pada keamanan informasi yang dikelola. Ancaman kejahatan siber, seperti pencurian identitas dan ransomware, menunjukkan perlunya kesadaran yang lebih tinggi di masyarakat mengenai perlindungan data pribadi.

Indonesia telah menginisiasi langkah-langkah melalui regulasi untuk melindungi data pribadi, namun tantangan dalam penegakan hukum dan kurangnya kesadaran masyarakat masih menjadi hambatan. Oleh karena itu, Kerja sama antara pemerintah, sektor non-negeri, dan masyarakat sangat esensial dalam mewujudkan kondisi yang aman bagi data pribadi. Kerjasama internasional juga diperlukan untuk menghadapi kejahatan siber yang semakin kompleks. Dengan upaya bersama dalam meningkatkan kesadaran dan regulasi, perlindungan data pribadi dapat terwujud, memastikan hak-hak individu tetap terjaga di tengah kemajuan teknologi yang pesat.

DAFTAR REFERENSI

- Ali, M. (2024). Analisis Peran ICC dalam Penuntutan Kejahatan Siber Crime Internasional dalam Praktik Hukum Pidana Internasional: Analisis Peran ICC dalam Penuntutan Kejahatan Siber Crime Internasional dalam Praktik Hukum Pidana Internasional. *Jurnal Hukum Lex Generalis*, 5(1).
- Aprianto, N. E. K. (2021). Peran teknologi informasi dan komunikasi dalam bisnis. *International Journal Administration, Business & Organization*, 2(1), 8–15.
- Azis, Y. A. (2023). *Studi Pustaka: Pengertian, Tujuan, Sumber dan Metode*.
- Danial, A. R. (2009). *Metode Penelitian Sastra: Pendekatan Kualitatif dan Kuantitatif*. Jakarta:

-
- Bumi Aksara.
- Edrisy, I. F. (2019). Pengantar Hukum Siber. Sai Wawai Publshing, IAIN Metro.
- Friese, M., Bürgler, S., Hofmann, W., & Hennecke, M. (2024). Self-regulatory flexibility. *Current Opinion in Psychology*, 60, 101878.
- Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, 4(2), 23–31.
- Jie, B., Eric, E., Mervyn, D., Anggrianto, V., Kelvin, K., & Gabriella, C. (2023). Pemanfaatan dan dampak penggunaan teknologi informasi pada bidang sosial. *Journal of Information System and Technology (JOINT)*, 4(2), 392–397.
- Khadam, N., Anjum, N., Alam, A., Ali Mirza, Q., Assam, M., Ismail, E. A. A., & Abonazel, M. R. (2023). How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. *Heliyon*, 9(12), e22823.
- Krisnan. (2021). 7 Pengertian Metode Penelitian Kualitatif Menurut Para Ahli.
- Mahardika, A. M. (2021). Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia. *Jurnal Hukum*, 37(2), 101–118.
- Mason, R. (2000). From distance education to online education. *The Internet and Higher Education*, 3(1–2), 63–74.
- Nguyen, D. C. L., & Golman, D. W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: “Law on the books” vs “law in action.” *Computer Law & Security Review*, 40, 105521. doi:10.1016/j.clsr.2020.105521
- Rakhmayanti, I. (2019). Data Boleh Disimpan di Luar Negeri, Ini Pembeneran versi Kominfo.
- Rosadi, S. D. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia*, 5(1), 35–53.
- Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia. *Aisyah Journal Of Informatics and Electrical Engineering (AJIEE)*, 5(2), 227–233.
- Stiawan, D. (2005). Sistem Keamanan Komputer. Elex Media Komputindo.
- Tandy, J., & Siswono, S. (2013). Cloud Computing dan Dampaknya Terhadap Bisnis. *ComTech: Computer, Mathematics and Engineering Applications*, 4(2), 687–695.
- Wardiana, W. (2002). Perkembangan teknologi informasi di Indonesia.