ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

RESEARCH ARTICLE

Upaya Hukum dalam Strategi Perlindungan Data pada Penggunaan Internet Studi Kasus : Hacker Bjorka

Annisa Nadya Putri✉

Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta

✉2110413034@mahasiswa.upnvj.ac.id

ABSTRACT

The hacking case committed by Bjorka has caused controversy and attracted public attention due to his hacking action against various important data and its dissemination through social media. This article aims to examine the legal remedies that can be applied in data protection strategies related to internet usage, with a focus on the Bjorka hacking case. The research discusses the legal and regulatory framework in Indonesia relevant to Bjorka's hacking actions. In addition, the author explores solutions and efforts that can be taken by the government, responsible institutions, and the public in tackling cybersecurity threats. This research uses a qualitative approach with literature review as the data collection method. The article is organized descriptively, integrating various primary and secondary data to support the analysis. By detailing the regulations of the ITE Law, the New Criminal Code, aspects of cybercrime, and the Bjorka hacking case, this research is expected to contribute to an in-depth understanding of the legal framework and data protection strategies in the digital era.

Keywords: *Bjorka hacking, Cybercrime, ITE Law, KUHP Baru.*

ABSTRAK

Kasus peretasan yang dilakukan oleh Bjorka telah menimbulkan kontroversi dan menarik perhatian publik karena aksi meretasnya terhadap berbagai data penting dan penyebarannya melalui media sosial. Artikel ini bertujuan untuk mengkaji upaya hukum yang dapat diterapkan dalam strategi perlindungan data terkait penggunaan internet, dengan fokus pada kasus peretasan oleh Bjorka. Penelitian ini membahas kerangka hukum dan regulasi di Indonesia yang relevan dengan tindakan peretasan Bjorka. Selain itu, penulis mengeksplorasi solusi dan upaya yang dapat diambil oleh pemerintah, lembaga yang bertanggung jawab, dan masyarakat dalam menanggulangi ancaman keamanan siber. Penelitian ini menggunakan pendekatan kualitatif dengan literature review sebagai metode pengumpulan data. Artikel ini disusun secara deskriptif, mengintegrasikan berbagai data primer dan data sekunder untuk mendukung analisis. Dengan merinci peraturan UU ITE, KUHP Baru, aspek-aspek kejahatan siber, dan kasus peretasan Bjorka, penelitian ini

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

diharapkan memberikan kontribusi pada pemahaman mendalam tentang kerangka hukum dan strategi perlindungan data di era digital.
Kata Kunci: Cybercrime, KUHP Baru, Peretas Bjorka, UU ITE.

PENDAHULUAN

Perkembangan teknologi informatika dan arus digitalisasi yang semakin masif memberi jalan pada keterbukaan informasi yang luas, keadaan ini memunculkan istilah dunia tanpa batas. Maka revolusi industri yang mendorong publik untuk masuk serta menghuni dunia siber dengan amat sangat kilat dan intensif. Kemunculan internet dari adanya perkembangan teknologi telah membentuk jaringan-jaringan yang menghubungkan manusia tanpa batas jarak dan waktu. Keadaan ini tentu dapat menjadi peluang dan secara bersamaan menimbulkan tantangan yang nyata bagi manusia. Secara peluang tentu, kita telah mengalami berbagai kemudahan dalam aktivitas sehari-hari dengan adanya perkembangan teknologi, khususnya dengan ada internet telah mampu menghubungkan manusia dengan jarak yang jauh. Dengan internet pula kita dapat mengakses berbagai informasi dengan mudah dan cepat. Akan tetapi, internet membawa kita pada suatu tantangan mengkhawatirkan akan adanya kerawanan kejahatan siber/cyber crime (Thomas & Adam, 2015). Internet dengan berbagai situs dan website kerap menyimpan data-data pribadi kita kedalam data milik mereka. Keamanan akan penyimpanan data internet yang masih rawan kerap memberi kesempatan bagi para Hacker untuk meretas suatu website yang kemudian mencuri data-data pribadi pengguna internet yang tersimpan pada sistem keamanan website. Salah satu permasalahan yang timbul beberapa waktu silam ialah terkait dengan kebocoran data, baik milik pemerintah maupun milik pribadi. Hal ini jelas memicu keresahan di masyarakat, yang dimana kebocoran ini adalah salah satu kekurangan untuk bagian penting dalam unsur perlindungan data pribadi. Berbagai kasus pencurian data pribadi telah banyak merugikan pengguna internet baik secara material maupun nonmaterial. Maraknya hal tersebut membawa perhatian kita pada keamanan dan perlindungan data pribadi dalam menggunakan internet. Pencanangan Revolusi Industri 4.0 di Indonesia juga telah masuk tahapan untuk mempersiapkannya. Perlu diketahui, dalam mempersiapkan Revolusi Industri 4.0 ini penting sekali dalam mengundangkan peraturan perlindungan data pribadi, sebab nantinya kegiatan yang dikerjakan manusia akan dikerjakan oleh komputer tanpa intervensi manusia dengan teknologi Artificial Intelligence (AI) yang didasarkan pada algoritma pekerjaan yang telah ditentukan.

Perlindungan akan data pribadi sejatinya menjadi hak asasi manusia yang mendasar, dimana data pribadi berkaitan dengan ranah privat seseorang atau disebut sebagai suatu privasi. Menurut Alan Westin (1967:7), privasi merupakan suatu klaim seseorang, kelompok, atau institusi untuk dapat menentukan kapan, bagaimana, sejauh mana informasi tentang mereka didistribusikan kepada orang lain. Kehadiran hacker bjorka pada tahun 2022 silam berhasil membuat publik terkejut dengan aksi kejahatan yang telah dilakukannya. Pasalnya, kemunculan hacker ini kerap menghilangkan sejumlah data pribadi dari penduduk Indonesia. Sebab bjorka mulai bergabung di Breached Forum pada bulan agustus tahun 2022 dengan memiliki predikat dewa karena kemahirannya dalam dunia hacker. Sehingga kepiawaian bjorka dalam melakukan aksi hacker terbilang sangat efektif dan terstruktur.

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

Karena tanpa ada satu orang pun yang dapat mengetahui identitas asli bjorka hingga penuh kontroversi baik di dunia digital maupun kehidupan dunia nyata. Bahkan pemerintah indonesia yang bekerja dalam bidang intelligent merasa sulit untuk menemukan identitas asli bjorka. Padahal pada praktiknya, aksi cyber yang dilakukan bjorka telah merugikan beberapa pihak terkait terutama dengan kelembagaan negara. Sebab data pribadi seluruh penduduk Indonesia berada di dalam kelembagaan tersebut dan tentu bersifat rahasia. Namun bjorka membuat kekacauan dengan mencuri hampir seluruh data milik perusahaan hingga lembaga pemerintahan negara dan beberapa data kepresidenan ataupun pejabat lainnya termasuk dengan BIN yang dibentuk untuk melindungi keamanan negara. Aksi kriminalitas bjorka ini dipandang oleh masyarakat indonesia termasuk berani dalam membongkar kegagalan pemerintah untuk mengamankan aset negara.

Maka adanya krisis legitimasi membuat kepercayaan publik menjadi turun sangat drastis. Hal ini dipicu oleh pengaruh dari sektor digitalisasi dan publik informasi yang terus tumbuh, serta ancaman dunia maya terbaru terus dirancang sedemikian rupa. Dengan begitu sudah kenyataannya untuk tidak diperkenankan internet atau website/platform yang menyimpan data diri pengguna internet menyebarluaskan data pribadi pengguna internet tersebut. Pada saat bersamaan internet pemilik website atau platform yang menyimpan data diri pengguna internet berkeharusan menjaga data-data tersebut untuk tidak tersebar atau dicuri oleh hacker. Selain itu, perlindungan data pribadi yang menjadi hak asasi manusia ini juga perlu diperhatikan oleh negara, sebab ini menjadi kewajiban negara untuk menjaga keamanan rakyatnya. Maka dari itu negara perlu memiliki aturan yang dapat memberi rasa aman bagi rakyatnya dalam menggunakan internet. Karena pengolahan data dalam jumlah besar, seperti data kependudukan serta data finansial hingga saat ini sepenuhnya mengenakan komputer.

Di Indonesia, dalam mengatur aktivitas internet telah terdapat UU Informasi dan Transaksi Elektronik yang sejatinya mengatur aktivitas penggunaan internet dan transaksi dengan menggunakan internet atau secara elektronik. Aturan tersebut rasa-rasanya belum mampu menghadirkan suatu perlindungan akan data pribadi pengguna internet di Indonesia. Maka kemudian terdapat tuntutan akan adanya peraturan yang lebih khusus mengatur perlindungan data pribadi dalam penggunaan internet. Akhirnya muncul UU PDP yang mengalami perjalan panjang hingga akhirnya disahkan. Namun UU PDP ini bukanlah jawaban satu-satunya terkait keamanan siber, kejahatan siber akan tetap merajalela tanpa adanya masyarakat digital yang teredukasi. Keadaan ini menuntut digalakkannya sosialisasi terkait edukasi dan literasi digital bagi masyarakat. Selain itu, penting pula bagi pemerintah untuk memberi standarisasi keamanan bagi website dan platform digital yang menyimpan data pribadi masyarakat. Terutama dengan keamanan cyber yang sudah menjadi titik fokus untuk konflik kepentingan dalam negeri dan internasional, serta terus menjadi guna proyeksi kekuatan negara. Peningkatan teknologi informasi telah memunculkan internet yang membawa pada keterbukaan akses informasi yang luas dan cepat. Arus digitalisasi telah meningkatkan kebutuhan manusia akan internet untuk dapat mempermudah aktivitas sehari-hari, akan tetapi internet telah membawa pada tantangan global terkait kejahatan siber. Kejahatan siber bukan hanya berbahaya bagi individu tetapi juga bagi negara, bahkan dunia internasional. Kejahatan siber terkait pencurian data pribadi sangat mengkhawatirkan bagi para pengguna internet. Berbagai kasus kebocoran data platform internet serta maraknya penjualan data pribadi oleh pada peretas atau hacker

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

membawa perhatian kita pada perlindungan data pribadi. Keadaan ini menjadi tantangan global yang menuntut negara untuk dapat melindungi data pribadi rakyatnya yang menggunakan internet. Masyarakat pengguna internet di dunia menuntut negara mereka memiliki aturan akan perlindungan data pribadi. Hal ini tidak terkecuali terjadi pula di Indonesia, dimana masyarakat menuntut aturan jelas dan pengesahan akan UU Perlindungan Data Pribadi. Selain dari adanya aturan, yang menjadi masalah terkait kejahatan siber di internet juga karena minimnya pengetahuan masyarakat tentang perkembangan teknologi informasi dan arus digitalisasi. Maka yang menjadi pertanyaan penelitian kami adalah:

a. Bagaimana Upaya Perlindungan Hukum Dalam Mengatasi Kasus Bjorka?
b. Bagaimana Strategi Dalam Mengamankan Atau Melindungi Data Pribadi Pada Penggunaan Internet?

METODE

2.1 Jenis Penelitian

Penulisan makalah ini menggunakan metode penelitian kualitatif dengan teknik pengumpulan data melalui literature review. Metode penelitian ini sendiri memiliki landasan berpikir dari Max Weber karena metode kualitatif sendiri memberikan penekanan terhadap pengamatan suatu peristiwa atau fenomena yang terjadi dengan lebih berfokus kepada substansi dari sebuah peristiwa atau fenomena yang terjadi tersebut. Dengan demikian, metode ini tidak memerlukan mekanisme perhitungan atau statistik dalam proses mengumpulkan datanya. Metode ini sendiri memiliki tujuan untuk mengerti serta memahami sebuah objek yang diteliti dengan cara yang lebih mendalam. Perlu diketahui bahwasannya dalam metode penelitian ini hasil yang didapatkan merupakan hasil dari penafsiran serta pemahaman berdasarkan hasil penalaran dari peneliti sendiri. Oleh karena itu, hasil dari metode penelitian ini merupakan sebuah bentuk pengembangan dari konsep sensitivitas dari sebuah permasalahan yang sedang dihadapi yaitu dengan menerangkan suatu keadaan realitas yang tersedia dan yang berkaitan dengan fenomena atau peristiwa yang dihadapi.

2.2 Sumber Data

Data sendiri merupakan sekumpulan fakta - fakta ataupun keterangan - keterangan yang diperoleh dan kemudian akan diolah dalam sebuah kegiatan penelitian yang dilakukan. Data menurut sumbernya terdiri dari dua jenis data yaitu data primer dan data sekunder, yang mana data primer dapat didapatkan dengan melalui proses langsung dari subjek yang diteliti atau yang biasa dikenal sebagai wawancara. Sedangkan data sekunder merupakan sekumpulan keterangan atau fakta - fakta diperoleh secara tidak langsung dimana data tersebut dikumpulkan dengan melalui cara yang tidak langsung atau dengan melalui perantara kedua seperti melalui media informasi yang tersedia baik itu melalui buku, jurnal, website, maupun berbagai bentuk dokumentasi relevan yang lainnya.

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

2.3 Teknik Pengumpulan Data

Metode kualitatif dengan pengumpulan data melalui literature review ini terdiri dari beberapa teknik pengumpulan yang mana salah satunya adalah dengan melalui studi dokumen. Metode studi dokumen sendiri merupakan suatu metode pengumpulan data dalam sebuah penelitian sosial sebagai upaya untuk mengumpulkan bukti - bukti data tertulis yang dapat ditemukan seperti melalui transkrip, catatan harian, buku, surat kabar, serta media penunjang lainnya seperti website, buku, jurnal serta berbagai bentuk dokumentasi relevan lainnya. Seperti yang diketahui bahwasannya dalam era globalisasi ini maka perkembangan teknologi informasi akan semakin pesat perkembangannya, oleh karena itu, studi dokumentasi menjadi salah satu bagian yang penting dan juga tidak dapat dipisahkan dengan metode penelitian kualitatif. Dalam artikel ilmiah ini kelompok kami menggunakan teknik pengumpulan data sekunder yaitu dimana kelompok kami tidak melakukan pengumpulan fakta dan juga keterangan secara langsung dengan melakukan wawancara melainkan kami melakukan pengumpulan fakta - fakta dan juga keterangan melalui perantara kedua yaitu dengan melalui website, jurnal, dan juga buku yang kelompok kami temukan.

2.4 Teknik Analisa Data

Dengan penggunaan metode penelitian kualitatif dengan pengumpulan data melalui literature review ini, maka dengan demikian hasil data yang dihasilkan akan berupa kalimat - kalimat pernyataan yang kemudian digunakan untuk menginterpretasikan makna serta pemahaman terkait dengan permasalahan yang sedang diteliti. Tahapan ini sendiri dilakukan selama proses penulisan penelitian. Dalam metode penelitian kualitatif, maka akan digunakan metode induktif yaitu dimana penelitian ini tidak akan melakukan pengujian terhadap hipotesis karena hipotesis hanya digunakan sebagai pedoman melainkan dengan melakukan penyusunan abstrak yang berdasarkan dengan temuan data - data yang ditemukan pada saat proses pengumpulan data – data lapangan selama proses pengumpulan data tersebut dilakukan. Analisis data yang terdapat di dalam metode penelitian ini kemudian akan dilakukan secara lebih intensif, karena analisis baru akan dilakukan setelah semua data dan informasi yang ditemukan dan dikumpulkan di lapangan dirasa sudah cukup dan memadai untuk diolah lalu kemudian disusun sampai dengan kesimpulan yang merupakan tahapan akhir dari penelitian. Seperti yang dilakukan oleh kelompok kami dimana kelompok kami berusaha untuk mengumpulkan data serta informasi - informasi dengan melakukan kegiatan reduksi yaitu berupaya untuk memilah apa saja hal - hal yang dirasa penting dari setiap data yang ditemukan di lapangan pada saat proses pengumpulan data sampai dengan tahapan laporan hasil.

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

HASIL DAN DISKUSI

3.1 Upaya Perlindungan Hukum Dalam Mengatasi Kasus Bjorka

Saat ini, kemajuan dan perkembangan teknologi informasi memberikan dampak yang besar bagi kehidupan sosial. Setiap lapisan masyarakat kini sangat bergantung pada teknologi dan komunikasi digital, termasuk media sosial, sebagai hasil dari kemajuan teknologi. Media sosial digunakan secara luas, dan dengan itu muncul kemudahan akses ke informasi, termasuk informasi pribadi dan isu-isu terkait privasi. Terlepas dari kenyataan bahwa data pribadi adalah komponen hak asasi manusia yang harus dilindungi, hal ini menyebabkan penyalahgunaan data pribadi selama interaksi di media sosial (Hanifan, 2020). Masyarakat berkembang dan berubah seiring dengan perkembangan teknologi. Penggunaan teknologi internet ditingkatkan dengan adanya globalisasi, yang membuka banyak prospek pengembangan baru dan memfasilitasi komunikasi dan berbagi informasi. Sebaliknya, hal ini menciptakan celah baru untuk gangguan privasi. Kekhawatiran akan gangguan privasi menyoroti betapa pentingnya melindungi informasi pribadi, terutama mengingat semakin banyaknya orang yang menggunakan ponsel pintar dan internet. Mewujudkan perlindungan data pribadi bagi setiap warga negara Indonesia adalah tujuan negara dalam lanskap teknologi informasi dan komunikasi saat ini. Privasi pada dasarnya adalah melindungi informasi pribadi. Kasus-kasus tersebut menyoroti perlunya langkah-langkah hukum untuk melindungi data pribadi, terutama yang melibatkan kebocoran data pribadi yang mengakibatkan beberapa tindakan penipuan atau tindakan ilegal seperti pornografi (Nasrudin & Latumahina, 2022). Masalah yang baru-baru ini terjadi adalah kebocoran data yang menyebabkan gejolak sosial dan berasal dari pemerintah maupun warga negara. Pelanggaran ini menunjukkan kelemahan serius dalam sistem perlindungan informasi pribadi.

Karena pada praktiknya, kebocoran data masih sering terjadi di Indonesia hingga sampai saat ini. Kasus kebocoran data yang belum lama ini terjadi adalah dimana salah satu hacker bernama Bjorka dilaporkan meretas data-data yang terdapat di BUMN, Kementerian bahkan data pribadi pejabat negara. Indonesia sendiri menempati posisi ke-3 sebagai negara yang memiliki kasus kebocoran data terbanyak di dunia menurut Surf Shark. Mereka mencatat adanya kebocoran data sebanyak 12,74 juta per 13 September 2022. Data pribadi seseorang seharusnya merupakan data privasi yang hanya dapat diakses oleh pengguna yang memiliki data tersebut, dan orang lain tidak memiliki wewenang untuk mengakses dan menggunakan data pribadi orang lain. Kebocoran data pribadi seseorang sendiri memiliki dampak yang dapat merugikan orang tersebut. Dampak ini tergantung dari seseorang yang berusaha memanfaatkan data tersebut. Salah satu dampaknya adalah data seperti NIK, alamat, nama, dan tanggal lahir yang diretas seseorang data digunakan untuk membuat akun pinjaman online. Penggunaan data seperti ini dapat dikategorikan sebagai pencurian identitas jika seseorang yang mengambil data tersebut melakukannya secara diam-diam. Pencurian identitas pribadi ini merupakan perbuatan kriminal yang mana tercatat dalam Pasal 35 UU No 11 tahun 2008 tentang ITE. UU tersebut merupakan suatu kebijakan yang dibuat oleh pemerintah mengenai aktivitas pencurian data elektronik (Nabilah, 2022). Sehingga aksi hacker bjorka ini termasuk ke pelanggaran pasal berlapis dalam aturan konstitusi Indonesia.

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

Sementara itu, kehadiran Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi juga menjadi titik awal yang menarik bagi berbagai pemangku kepentingan, mulai dari pemerintah, perusahaan, hingga individu. Undang-undang ini mengubah lanskap hukum di Indonesia terkait perlindungan data pribadi dan memiliki dampak yang signifikan pada berbagai sektor ekonomi dan masyarakat. Pada sebelumnya peraturan UU ini kerap menggantikan Undang-Undang No. 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik, yang telah menjadi acuan hukum terkait perlindungan data pribadi pada kebijakan sebelumnya. Maka dari itu, perlu adanya kesadaran dan perhatian dari pemerintah pusat terkait upaya dalam penyelesaian dari konflik kebocoran data pribadi ini. Karenanya akan ada ambiguitas hukum, tumpang tindih antara peraturan yang relevan, kekacauan di dalam setiap sektor karena kepentingan yang saling bersaing, dan perasaan tidak terlindungi secara memadai oleh masyarakat secara keseluruhan jika peraturan perundang-undangan tidak diselaraskan. Agar Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) dapat menjadi bagian dari salah satu Program Legislasi Nasional Prioritas Pemerintah tahun 2021. Dengan begitu, urgensi pembuatan dalam aturan perundang-undangan saat ini telah tercapai tujuannya untuk menyelesaikan kasus hacker bjorka walaupun tidak sampai tuntas.

3.2 Relevansi Hukum dan Regulasi Indonesia Terkait Kasus Hacker Bjorka

Selama akhir Agustus dan awal September 2022, salah satu contoh yang paling menonjol adalah peretasan dan pembelian serta penjualan data menggunakan akun anonim dengan nama Bjorka. Dia menjual informasi pribadi, catatan publik yang sensitif, dan informasi pribadi beberapa pemimpin negara. Mulai dari data-data pemerintah, hingga informasi pribadi sejumlah petinggi negara. Informasi mengenai perdagangan data pribadi dan bocornya 26 juta data pelanggan Indihome yang beredar di kalangan pengguna internet menandai awal mula aktivitas peretasan tersebut. Informasi pelanggan Indihome diperjualbelikan di situs Breached Forums. Kemudian, 1,3 miliar nomor kartu SIM pelanggan ponsel terekspos oleh kebocoran tersebut. Dilaporkan bahwa informasi tersebut diperoleh dari penyedia layanan telekomunikasi menjelang akhir Agustus. Setelah itu, enam hari kemudian, akun Bjorka mengiklankan 105 juta data statistik kependudukan yang diklaim diperoleh dengan meretas situs KPU. Tidak hanya itu, pada Sabtu, 9 Oktober 2022, Bjorka muncul kembali dan menyatakan telah mengunduh 679.180 dokumen dan catatan resmi negara. Beberapa dokumen berlabel rahasia yang diterima Presiden Joko Widodo diunggah olehnya. Selain itu, Bjorka juga mengunggah informasi pribadi milik pejabat negara lainnya. Di antaranya adalah Ketua DPR RI Puan Maharani, Menteri Badan Usaha Milik Negara (BUMN) Erick Thohir, dan Menteri Komunikasi dan Informatika (Menkominfo) Johnny G. Plate.

Pelanggaran-pelanggaran yang dilakukan oleh hacker bjorka bersinggungan dengan hukum dan regulasi Indonesia yang mengatur tentang cybercrime. Dalam menanggulangi dan juga pemberlakuan hukum terhadap hacker bjorka, terdapat beberapa lembaga dan pihak yang memiliki wewenang - Kementerian Komunikasi dan Informatika (KOMINFO), Pihak Penyelenggara Sistem dan Transaksi Elektronik (PSTE), Pihak Kepolisian, Badan Intelijen Negara (BIN) serta Badan Sandi dan Sandi Negara (BSSN). Sejumlah pasal dalam

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

undang-undang Indonesia, khususnya Undang-Undang Nomor 19 Tahun 2016 yang memuat Informasi dan Transaksi Elektronik (UU ITE), mengatur kegiatan seperti peretasan dan kejahatan siber, yang mana itulah yang dilakukan oleh peretas BJORKA. Pasal 30 dan Pasal 47 UU ITE, yang sekarang diuraikan dalam Pasal 258 KUHP Baru (KUHP Baru), menetapkan bahwa setiap orang yang menggunakan jaringan kabel komunikasi atau jaringan nirkabel untuk secara melawan hukum melakukan intersepsi, perekaman, pengubahan, pengacauan, dan/atau pencatatan Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat non-publik dapat diancam dengan pidana penjara paling lama 10 tahun atau pidana denda paling banyak kategori IV. Demikian pula, hukuman penjara maksimum 10 tahun atau hukuman kategori IV dapat dikenakan untuk menyebarluaskan atau menyiarkan temuan intersepsi atau perekaman tersebut. Namun, seperti yang dinyatakan dalam Pasal 31 dan 32, larangan-larangan ini tidak berlaku untuk individu yang menjalankan instruksi resmi atau persyaratan undang-undang.

Pasal 332 UU ITE, yang juga terkait dengan Pasal 30 dan 46, menyatakan bahwa setiap orang yang dengan sengaja dan tanpa izin atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan tujuan tertentu dapat dipidana dengan pidana penjara paling lama enam tahun atau pidana denda paling banyak kategori V. Hal ini berkaitan dengan akses tidak sah ke komputer dan/atau sistem elektronik milik orang lain. Selain itu, pelaku dapat dikenakan hukuman penjara maksimal tujuh tahun atau hukuman kategori V jika akses tidak sah tersebut dilakukan dengan maksud untuk mendapatkan informasi atau dokumen elektronik. Akses tidak sah yang melanggar sistem keamanan dapat dikenai hukuman maksimal delapan tahun penjara atau denda kategori VI.

Selain undang-undang tentang peretasan, Peraturan Presiden No. 53 tahun 2017 mengatur Badan Siber dan Sandi Negara (BSSN) di Indonesia. BSSN bekerja sama dengan penegak hukum, khususnya Direktorat Kejahatan Siber Kepolisian Republik Indonesia, untuk menanggapi kejadian peretasan. UU No. 36 Tahun 1999 tentang Telekomunikasi; UU No. 19 Tahun 2002 tentang Hak Cipta; UU No. 15 Tahun 2003 tentang Telekomunikasi; UU No. 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme; UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; dan UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 adalah beberapa dari beberapa undang-undang yang digunakan oleh pemerintah dalam upayanya untuk memerangi peretasan. Namun demikian, masih ada beberapa masalah dan batasan dengan cara KUHP menangani perkembangan teknis dan pelanggaran teknologi tinggi.

Selain itu, KUHP pada umumnya bersifat konvensional dan tidak secara langsung berkaitan dengan meningkatnya kejahatan siber dan pertumbuhan kriminalitas online. Kemungkinan adanya lebih banyak kejahatan harus dipertimbangkan dalam memerangi kejahatan ini, serta bagaimana penegak hukum dapat menggunakan informasi ini untuk membuat aturan yang efisien. Asas culpabilitas yang menyatakan bahwa tidak ada hukuman tanpa kesalahan ini diakui oleh hukum Indonesia. Asas ini harus dipertimbangkan dalam proses pidana yang melibatkan kejahatan siber. Hal ini dimaksudkan agar penegak hukum dapat lebih berhati-hati dalam menentukan kesalahan pelaku kejahatan peretasan. Setiap strategi hukum pidana yang bertujuan untuk memerangi kejahatan siber harus mempertimbangkan nilai-nilai. Nilai-nilai harus diperhitungkan dalam masalah siber. Sebagai akibat dari kesulitan dalam mengidentifikasi dan membuktikan adanya unsur kesalahan, kemungkinan pengguna melintasi batas negara, kesulitan dalam mengidentifikasi

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

mereka secara akurat, dan lingkungan digital di mana mereka ditemukan, lembaga-lembaga siber di Indonesia mungkin menemukan kesulitan dalam menangani masalah ini ketika datang ke implementasi.

3.3 Strategi Dalam Melindungi Data Pribadi Pada Penggunaan Internet

Sebagai negara yang sedang berkembang, Indonesia memiliki populasi yang cukup besar yang memanfaatkan komunikasi dan teknologi kontemporer. Namun, saat ini, Indonesia tidak memiliki undang-undang khusus yang mengatur privasi informasi pribadi. Pada kenyataannya, peraturan-peraturan ini tidak cukup untuk memberikan keamanan yang memadai terhadap eksploitasi informasi pribadi, terutama di media elektronik seperti platform media sosial, dan terutama ketika penyalahgunaan tersebut mengakibatkan kejahatan yang lebih serius atau tindakan kriminal lainnya. Jelaslah bahwa hak privasi, yang mencakup kebebasan untuk menjalani kehidupan pribadi seseorang tanpa gangguan dan hak untuk mengatur akses ke informasi tentang kehidupan pribadi seseorang, termasuk hak atas data pribadi. Individu memiliki hak untuk memilih apakah akan menukar atau membagikan data pribadinya, sesuai dengan pengertian perlindungan data pribadi (Nurhidayati, Sugiyah, & Yuliantari, 2021). Namun, kekhawatiran tentang pelanggaran informasi pribadi baru-baru ini, seperti kasus Bjorka, muncul lagi. Di dunia yang ideal, negara akan diwajibkan oleh Undang-Undang Hak Asasi Manusia untuk melindungi data pribadi warganya, karena masyarakat modern sangat bergantung pada peraturan tersebut. Meningkatnya penggunaan data pribadi dalam transaksi berbasis teknologi di berbagai aspek kehidupan memunculkan sejumlah masalah. Regulasi yang mengatur masyarakat terhadap berbagai masalah yang berkaitan dengan eksploitasi data pribadi dalam pemanfaatan teknologi informasi sayangnya masih sangat minim hingga tulisan ini dibuat. Hak untuk menghormati kehidupan pribadi, yang terkadang disebut sebagai "the right to private life", memunculkan hak atas perlindungan data pribadi.

Maka dari itu, selain adanya UU ITE kini Indonesia juga mengeluarkan rancangan UU PDP atau Undang-Undang Perlindungan Data Pribadi. Yang mana Undang-Undang tersebut dibuat karena melihat bagaimana banyak data pribadi masyarakat Indonesia yang bocor. UU ini diharapkan dapat menjamin keamanan data pribadi masyarakat Indonesia dan memberikan hak masyarakat atas perlindungan data pribadi mereka. Perlindungan data pribadi merupakan salah satu hak asasi manusia dan tercantum dalam Pasal 28G UUD 1945. Tetapi UU ini baru akan ditandatangani oleh presiden pada bulan Oktober dan disahkan pada bulan September. Meskipun, UU ini dibuat untuk melindungi data pribadi masyarakat, tetapi meminimalisir resiko kebocoran data pribadi merupakan tanggung jawab bersama antara pemerintah dan masyarakat. Di satu sisi pemerintah memiliki tugas yang sangat berat dalam mengimplementasikan UU ini. Tugas pemerintah tidak hanya membuat UU saja, mereka juga harus dapat mengedukasi masyarakat akan data pribadi mereka. Hal ini dikarenakan masih banyak ditemukan masyarakat Indonesia yang memberikan data pribadi mereka kepada seseorang entah karena paksaan atau alasan lainnya. RUU Perlindungan Data Pribadi Pasal 1 Ayat 1 mendefinisikan data pribadi sebagai setiap informasi tentang seseorang, baik yang diperoleh secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik, dan apakah informasi tersebut diidentifikasi dan/atau

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

dapat diidentifikasi secara tersendiri atau digabungkan dengan informasi lain (Shandy & Sari, 2023).

Alinea keempat Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menjelaskan dan menekankan kewajiban konstitusional negara Indonesia, yang meliputi melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan keadilan sosial, kemerdekaan, dan perdamaian abadi. Negara ingin memastikan bahwa data pribadi seluruh penduduk Indonesia terlindungi di tengah perkembangan teknologi informasi dan komunikasi saat ini. Pada dasarnya, salah satu aspek dari privasi adalah perlindungan terhadap informasi pribadi. Gagasan privasi adalah untuk melindungi integritas dan martabat pribadi setiap orang. Istilah lain yang diadopsi kemudian oleh negara-negara maju untuk menyebut data pribadi sebagai hak yang perlu dijaga adalah privasi, yang merupakan hak individu untuk tidak diganggu kehidupan pribadinya. Mengeksplorasi privasi berarti mengeksplorasi kebebasan untuk menjalani kehidupan yang memuaskan. Meskipun diakui sebagai hak asasi manusia yang mendasar, privasi adalah gagasan yang sulit untuk didefinisikan dan berubah tergantung pada situasi, negara, dan budaya. Perlindungan data dan hak atas privasi merupakan komponen penting dari otonomi dan martabat pribadi. Realisasi kebebasan yang berkaitan dengan politik, agama, spiritualitas, dan bahkan kehidupan pribadi didorong oleh perlindungan data. Tiga hak dasar-privasi, kebebasan berbicara, dan penentuan nasib sendiri-memberikan manusia hak-hak intrinsik yang kita miliki sejak lahir.

Dalam konteks keamanan siber, segala faktor penduduk wajib ikut serta di dalam proses formulasi serta penerapan strategi keamanan siber. Tentu saja hal tersebut, kepemimpinan politik senantiasa memegang peranan terutama dalam perihal ini. Mengenai keamanan siber tidaklah hanya perkara politik serta keamanan satu negara semata. Kedatangan dan pertumbuhan dunia siber selaku sistem pengolahan data serta komunikasi secara massal tidak cuma menguntungkan banyak negara, namun pula sebagai resiko keamanan yang besar. Oleh karena itu, masih banyak strategi lainnya untuk melindungi data pribadi masyarakat. Yang mana dapat dilihat website-website di Indonesia masih belum menerapkan two factor authentication yang mana ini merupakan lapisan pengamanan data diri seseorang dengan memberikan notifikasi saat ada orang lain yang ingin masuk ke dalam akun orang tersebut (Muin, 2023). Selain itu kita juga dapat menerapkan sistem barcode yang mana kita dapat masuk kedalam akun yang kita miliki hanya dengan menscan barcode tersebut untuk meminimalisir memasukan email dan password yang bisa jadi terbaca oleh hacker merujuk pada pasal 26 UU ITE yang menegaskan bahwa penggunaan informasi elektronik apapun di media harus dengan persetujuan pemilik data tersebut. Jika data pribadi disalahgunakan tanpa persetujuan pemiliknya, maka pemiliknya dapat menempuh jalur hukum, yaitu dengan menggugat kerugian yang ditimbulkan seperti yang tertera pada Pasal II ayat 2 yang berbunyi, "Setiap orang yang haknya dilanggar sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan ganti rugi atas kerugian yang ditimbulkan berdasarkan undang-undang ini." Maka kekuatan siber tidak bergantung pada sumber daya militer, tetapi pada kehadiran orang-orang yang menguasai programming sistem siber dan mampu menerapkannya sesuai keperluan. Dengan kekuatan siber yang besar, sebuah negara bisa memiliki pengaruh besar di dalam politik global. Namun disisi lain, eksistensi satu orang yang mendominasi sistem siber, maka hal tersebut dapat menjadi senjata yang amat

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

berbahaya bagi suatu negara walaupun negara tersebut memiliki sumber daya militer yang termasuk kecil.

Tidak hanya itu setiap website atau app harus memiliki fitur recovery data, yang mana pengguna bisa mengambil kembali data mereka yang sudah dicuri dan juga pengguna dapat tahu apa saja data mereka yang dicuri oleh hacker tersebut. Notifikasi ini dapat dikirimkan langsung ke dalam email sang pengguna agar mereka dapat mengeceknya secara langsung. Di tambah juga fitur pendeteksi dimana sang hacker berada seperti negara, dan kapan akun mereka diretas. Di tambah juga fitur pendeteksi dimana sang hacker berada seperti negara, dan kapan akun mereka diretas. Karena adanya perkembangan teknologi di era 4.0 pada saat ini yang diibaratkan sebuah pedang bermata dua. Manusia dapat merasakan manfaat dari adanya kemajuan teknologi untuk memudahkan hidup, tetapi kemajuan teknologi pula dapat melahirkan sebuah ancaman baru terhadap data pribadi kita. Di sisi lain, diperlukannya juga pembentukan sebuah lembaga baru selain KOMINFO layaknya KPK dan juga Komnas HAM yang dapat menaungi permasalahan mengenai kehilangan atau kebocoran data pribadi seperti yang tertuang dalam pasal 58 UU PDP yang menyatakan bahwasannya penyelenggaraan perlindungan data pribadi adalah peran dari pemerintah melalui lembaga dimana lembaga baru yang mana lembaga tersebut dibentuk oleh peraturan presiden serta bertanggung jawab kepada presiden dan diatur dalam peraturan presiden. Tujuan dari pembentukan peraturan perundang-undangan kini telah tercapai. Tujuan dibuatnya RUU PDP adalah untuk memberikan kejelasan dan jaminan hukum kepada Warga Negara Indonesia (WNI) sebagai pemilik data pribadi. Akan ada ketidakjelasan hukum, tumpang tindih antar peraturan yang terkait, kekacauan antar sektor untuk kepentingannya masing-masing, dan perasaan tidak didukung oleh masyarakat jika peraturan perundang-undangan tidak diharmonisasi.

KESIMPULAN

Majunya teknologi di Indonesia mendorong pula kemajuan baik dalam komunikasi dan informasi yang dimana bila kita berbicara tentang informasi maka kita akan mengenal lebih dalam tentang apa saja yang ingin kita ketahui tanpa harus dibatasi. Kebebasan dalam mencari informasi yang kita inginkan sangatlah menguntungkan bagi kita karena kita dapat mengetahui apa yang kita cari dan apa yang kita inginkan akan tetapi kebebasan dalam mencari informasi juga haruslah dibatasi dalam hal-hal tertentu seperti halnya data pribadi yang sebenarnya tidak dapat diketahui oleh banyak orang, karena data pribadi sangat sensitif untuk diketahui banyak orang. Tentu saja data pribadi tidak boleh dibagikan kepada banyak orang karena ditakutkan data pribadi dapat digunakan untuk kegiatan-kegiatan yang tidak jelas atau bisa saja digunakan untuk melakukan suatu pelanggaran atau tindak pidana. Dalam perkembangan Revolusi Digital 4.0 dan semakin ramainya platform yang membutuhkan akses data pribadi sudah seharusnya penyelenggara platform tersebut memberikan jaminan kerahasiaan terhadap setiap pengguna atau pemilik data pribadi tersebut. Perolehan dan pengumpulan data pribadi oleh penyelenggara sistem elektronik tersebut harus berdasarkan persetujuan atau berdasarkan ketentuan peraturan perundang - undangan. Menjadi sebuah keharusan bahwa pemerintah dapat memberikan perlindungan data pribadi kepada warga negaranya.

ISSN (Print) 2338-1051, ISSN (Online) 2777-0818

Akan tetapi dalam perkembangannya, aksi pencurian data pribadi dapat menimbulkan konsekuensi hukum. Seperti halnya dengan Kasus Bjorka yang sempat membuat geger dan telah melanggar beberapa aturan hukum konstitusi negara indonesia. Sebuah kejahatan siber penting ini yang terjadi pada akhir Agustus dan awal September 2022 melibatkan peretas Bjorka, yang memperdagangkan data sensitif, termasuk 26 juta data pelanggan Indihome, melalui peretasan. Pelanggaran yang dilakukan Bjorka sesuai dengan peraturan perundang-undangan di Indonesia, termasuk UU ITE. Peretasan dilarang oleh Pasal 30 dan 47 UU ITE, yang sekarang menjadi bagian dari KUHP Baru. Pelanggaran terhadap undang-undang ini dapat dikenai denda hingga kategori IV atau hukuman penjara hingga 10 tahun. Akses tidak sah ke komputer dapat dihukum hingga delapan tahun penjara atau denda kategori V hingga VI, menurut UU ITE Pasal 332. Untuk menegakkan peraturan ini, Indonesia memiliki organisasi seperti KOMINFO, PSTE, Kepolisian, BIN, dan BSSN. Terlepas dari kenyataan bahwa undang-undang ini menangani kejahatan siber, masih ada masalah dalam memperbarui undang-undang untuk mencerminkan teknologi baru. Untuk memberikan penilaian yang cermat terhadap kesalahan dalam situasi kejahatan siber, prinsip kesalahan sangat penting. Pengendalian kejahatan siber yang efektif membutuhkan keseimbangan antara taktik hukum ini dengan nilai-nilai dan menangani masalah lintas batas.

Sudah sepatutnya menjadi tamparan bagi pemerintah untuk lebih menguatkan keamanan data baik milik masyarakat maupun milik negara. Rancangan Undang-Undang Perlindungan Data Pribadi sudah terbilang sebagai langkah yang tepat, namun harus diiringi dengan siasat atau strategi lain; dalam hal ini untuk memerangi hacker atau bahkan cracker yang ingin merusak tatanan data seluruh warga Indonesia. Maka rancangan UUD ini termasuk ke dalam salah satu Program Legislasi Nasional Prioritas 2021. Sehingga urgensi pembuatan peraturan RUU PDP telah tercapai tujuannya. Adapun perancangan RUU PDP ini guna terciptanya kepastian hukum dan jaminan hukum bagi pemilik data pribadi, dalam hal ini Warga Negara Indonesia (WNI). Selain itu, sistem jaringan komputer juga perlu terus ditingkatkan sesuai dengan perkembangan terbaru agar keamanan siber tetap terjaga. Ruang siber yang aman akan membuat semua pengelolaan informasi menjadi efisien. Hal ini memudahkan semua orang untuk bekerja di berbagai bidang kehidupan, yang nantinya juga berujung pada peningkatan pertumbuhan ekonomi.

DAFTAR PUSTAKA

Hari, M. (2005). *Cybercrime. Dinamik*, 10(1).

Marx, K. (2018). *Capital Volume 1*. Lulu. Com.

Muin, I. (2023). Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia. *Journal Law And Justice*, *1*(2).

Nabilah, W., Putri, D., Rizal, D., and Warman, A. B. (2022). Implikasi Undang-Undang Informasi dan Transaksi Elektronik (UU-ITE) terhadap Kerukunan Kehidupan Beragama di Ruang Digital. *Dialog*, *45*(1), 69-80.

Nasrudin, F. K., and Latumahina, R. E. (2022). Perlindungan Hukum Terhadap Konsumen Kartu Sim Yang Mengalami Kebocoran Data Akibat Peretasan. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *2*(1), 331-343.

Negara, B. S. dan S. *Pasal 2 Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 Tentang*

Badan Siber dan Sandi Negara (2017). Retrieved from https://peraturan.bpk.go.id/Details/72920/perpres-no-53-tahun-2017

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis*, *7*(1), 105-119.

Nurhidayati, N., Sugiyah, S., and Yuliantari, K. (2021). Pengaturan perlindungan data pribadi dalam penggunaan aplikasi Pedulilindungi. *Jurnal Khatulistiwa Informatika*, *5*(1), 39-45.

Petrus, G. R. (2009). *Deradikalisasi Terorisme: Humanis, Soul Approach Dan Menyentuh Akar Rumput*.

Presiden Republik Indonesia. (2023). Undang-undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana. Direktorat Utama Pembinaan Dan Pengembangan Hukum Pemeriksaan Keuangan Negara Badan Pemeriksa Keuangan, (16100), 1–345.

Rizaldi, M. Z., Putra, R. D., and Hosnah, A. U. (2023). Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data. *Jurnal Justitia: Jurnal Ilmu Hukum dan Humaniora*, *6*(2), 619-627.

Robert. J. (2015). *Psychological Testing: History, Principles, And Applications*. United States Of America: Pearson Education Limited.

Shandy, R., and Sari, R. D. P. (2023). Aspek Hukum Pencantuman Data Pribadi Secara Sepihak Sebagai Kontak Darurat Dalam Perjanjian Kredit Online. *Binamulia Hukum*, *12*(1), 39-45.

Thomas, H., and Adam, B. (2015). *Cybercrime In Progress: Theory And Prevention Of Technology-Enabled Offenses*. Routledge.

Westin, A. F. (1967). Privacy and Freedom London: Bodley head. *WestinPrivacy and Freedom1967*.

Wijoseno, B. A., and Widhiyaastuti, I. G. A. A. D. (2023). Jerat Pidana Terhadap Pelaku Peretas Sistem Komputer Secara Ilegal (Hacker) Dalam Perpsektif Hukum Pidana Indonesia. *Jurnal Kertha Desa*, *11*(3), 2031-2041..