Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 8 Nomor 4, 2025
P-2655-710X e-ISSN 2655-6022

Submitted : 29/11/2025
Reviewed : 01/12/2025
Accepted : 01/12/2025
Published : 05/12/2025

Deva Inggria[1]
Wayne Gladys Octatiana Bella[2]
Asmak Ul Hosnah[3]

PENEGAKAN HUKUM TERHADAP TINDAK PIDANA CYBERCRIME DALAM KASUS PERETASAN DAN PELANGGARAN DATA PRIBADI OLEH HACKER BJORKA

Abstrak
Kasus kejahatan siber yang dilakukan oleh Bjorka menjadi salah satu peristiwa penting dalam sejarah keamanan digital Indonesia karena mengungkap lemahnya sistem perlindungan data pribadi dan infrastruktur keamanan siber nasional. Penelitian ini bertujuan untuk menganalisis bentuk tindak pidana cybercrime yang dilakukan oleh Bjorka serta penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam penegakan hukumnya. Metode yang digunakan adalah pendekatan yuridis normatif dengan menelaah peraturan perundang-undangan, literatur, serta data sekunder yang relevan. Hasil penelitian menunjukkan bahwa Bjorka melakukan berbagai bentuk tindak pidana siber seperti akses ilegal, pencurian dan penyebarluasan data pribadi, serta pemerasan dan gangguan terhadap sistem elektronik yang dapat dijerat melalui pasal-pasal dalam UU ITE dan UU PDP. Penerapan kedua undang-undang tersebut secara kumulatif memberikan dasar hukum komprehensif, namun masih menghadapi kendala implementatif seperti keterbatasan kapasitas aparat penegak hukum, belum optimalnya koordinasi antar lembaga, dan belum operasionalnya Lembaga Pelindungan Data Pribadi. Penelitian ini menegaskan pentingnya sinergi antara UU ITE dan UU PDP disertai penguatan kelembagaan, harmonisasi regulasi, serta peningkatan kapasitas penegakan hukum agar mampu mewujudkan perlindungan data pribadi dan keamanan digital yang berkelanjutan di Indonesia.
Kata kunci: Cybercrime; Perlindungan Data Pribadi; Penegakan Hukum.

Abstract
The cybercrime case committed by Bjorka has become one of the most significant events in the history of digital security in Indonesia because it revealed the weakness of the personal data protection system and national cyber security infrastructure. This study aims to analyze the forms of cybercrime committed by Bjorka and the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and Law Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) in law enforcement. The method used is a normative juridical approach by examining legislation, literature, and relevant secondary data. The results of the study show that Bjorka committed various forms of cybercrime, such as illegal access, theft and dissemination of personal data, as well as extortion and interference with electronic systems, which can be charged under articles in the ITE Law and PDP Law. The cumulative application of these two laws provides a comprehensive legal basis, but still faces implementation obstacles such as the limited capacity of law enforcement officials, suboptimal coordination between institutions, and the Personal Data Protection Agency not yet being operational. This study emphasizes the importance of synergy between the ITE Law and the PDP Law, accompanied by institutional strengthening, regulatory harmonization, and increased law enforcement capacity in order to be able to effectively protect personal data. This study emphasizes the importance of synergy between the ITE Law and the PDP Law, accompanied by institutional strengthening,

[1,2,3]Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pakuan Bogor
email: devainggria@gmail.com, waynegladys5@gmail.com, asmak.hosnah@unpak.ac.id

regulatory harmonization, and increased law enforcement capacity in order to realize sustainable personal data protection and digital security in Indonesia.
Keywords: Cybercrime; Personal Data Protection; Law Enforcement.

PENDAHULUAN

Perkembangan globalisasi dan kemajuan teknologi informasi telah merevolusi cara hidup manusia secara mendasar, membawa dampak transformatif dalam berbagai aspek kehidupan masyarakat di tingkat global. Perkembangan teknologi informasi dan komunikasi (TIK) yang semakin pesat tidak hanya memberikan kemudahan dalam mengakses informasi dan melakukan transaksi elektronik, tetapi juga menciptakan tantangan baru berupa kejahatan yang memanfaatkan teknologi sebagai sarana utamanya. Fenomena ini menandai berakhirnya era globalisasi konvensional dan dimulainya era digital yang membawa konsekuensi hukum dan sosial yang kompleks. Kemajuan Kemajuan teknologi informasi dan komunikasi telah membawa pengaruh yang signifikan terhadap beragam bidang kehidupan masyarakat, termasuk dalam sektor perbankan serta menjaga keamanan dan kerahasiaan data pribadi. Di era digital ini, kemudahan akses informasi dan transaksi elektronik memberikan manfaat besar, namun di sisi lain turut memunculkan potensi terjadinya kejahatan siber (cybercrime) yang semakin rumit dan merugikan. Kejahatan siber dapat didefinisikan sebagai setiap tindakan kriminal yang melibatkan penggunaan komputer atau jaringan internet sebagai alat, target, maupun lokasi kejahatan. Budi Suharyanto menegaskan bahwa kejahatan teknologi informasi atau cybercrime merupakan dampak tidak terduga dari globalisasi yang menjadi pendorong dimulainya era teknologi informasi.

Salah satu jenis kejahatan siber yang paling berbahaya adalah peretasan sistem informasi dan pencurian data pribadi, yang menimbulkan kerugian tidak hanya secara materiil tetapi juga mengancam kepercayaan publik terhadap institusi, khususnya lembaga pemerintahan dan keuangan. Statistik menunjukkan bahwa kejahatan siber di Indonesia mengalami peningkatan signifikan, dengan Bareskrim Polri melalui Pusiknas mencatat 14.867 kasus manipulasi data elektronik sejak Januari sampai 26 Oktober 2025, dengan rata-rata lebih dari 1.000 kasus per bulan. Polda Metro Jaya tercatat sebagai satuan kerja yang melakukan penindakan paling banyak, yakni 7.486 kasus, diikuti Sumatra Utara dengan 1.703 kasus dan Jawa Timur dengan 1.103 kasus. Merespons maraknya kejahatan siber, pemerintah Indonesia telah mengembangkan kerangka hukum yang komprehensif untuk menangani berbagai bentuk tindak pidana teknologi informasi. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diubah melalui UU Nomor 19 Tahun 2016 dan terakhir melalui UU Nomor 1 Tahun 2024, merupakan instrumen hukum utama dalam menangani kejahatan siber di Indonesia. Peraturan perundang-undangan ini memberikan prinsip hukum baru dan konsekuensi pidana yang diperluas, menjadikan tindakan yang sebelumnya tidak ilegal menjadi tindak pidana dengan sanksi tegas.

Dalam konteks perlindungan data pribadi, Indonesia telah mengundangkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengatur mekanisme pidana, administrasi, dan perdata dalam penegakan hukum terhadap pelanggaran data pribadi. UU PDP menetapkan sanksi pidana bagi siapa pun yang secara secara melanggar hukum mengambil atau menghimpun data pribadi untuk keuntungan pribadi maupun pihak lain, dengan ancaman pidana penjara hingga 5 tahun dan denda sebesar Rp5 miliar sebagaimana tercantum dalam Pasal 65 ayat (1) jo Pasal 67 ayat (1). Namun, implementasi UU PDP masih menghadapi tantangan serius karena pemerintah belum membentuk Peraturan Pemerintah dan otoritas pengawas PDP, sehingga banyak kasus pelanggaran data pribadi yang mandek dan tidak ditangani sampai tuntas. Salah satu kasus yang menggambarkan kompleksitas kejahatan siber di Indonesia adalah kasus yang melibatkan hacker berinisial WFT, yang dikenal dengan akun @bjorkaindonesia atau Bjorka. Kasus ini merupakan contoh nyata dari ancaman serius terhadap kedaulatan data nasional dan keamanan informasi publik. Dalam kasus ini, pelaku tidak hanya mengklaim berhasil meretas sistem perbankan dengan 4,9 juta akun nasabah, tetapi yang lebih mengkhawatirkan adalah peretasan terhadap basis data pemerintah yang mencakup jutaan data pribadi warga negara Indonesia dari berbagai instansi strategis seperti Direktorat Jenderal Imigrasi, BPJS Kesehatan, dan sistem registrasi kartu SIM.

Modus operandi Bjorka yang memanfaatkan dark web untuk memperoleh, menjual, dan menyebarluaskan data ilegal menunjukkan tingkat kecanggihan kejahatan siber yang semakin mengkhawatirkan dan mengancam stabilitas keamanan nasional. Bjorka tidak hanya melakukan pencurian data, tetapi juga melakukan pemerasan terhadap pemerintah dengan mengancam akan terus membocorkan data sensitif jika tuntutannya tidak dipenuhi, serta melakukan intimidasi publik melalui berbagai pernyataan provokatif yang merendahkan kapabilitas keamanan siber Indonesia. Penangkapan Bjorka pada Selasa, 23 September 2025, di Minahasa, Sulawesi Utara, menandai berakhirnya aksi kejahatan siber yang telah berlangsung selama bertahun-tahun dan menimbulkan keresahan massal di masyarakat. Pelaku dikenakan beberapa pasal dalam UU ITE dengan ancaman pidana maksimal 12 tahun penjara dan denda hingga Rp12 miliar, yang menunjukkan keseriusan negara dalam menangani kejahatan siber yang mengancam kedaulatan data dan privasi warga negara.

Aspek penting dalam penegakan hukum cybercrime adalah pemahaman terhadap elemen-elemen tindak pidana yang harus dipenuhi. Dalam konteks UU ITE, khususnya terkait dengan peretasan dan penyalahgunaan data, terdapat beberapa unsur yang harus dibuktikan, yaitu unsur kesengajaan (dolus), tanpa hak, dan perbuatan yang melanggar hukum baik berupa akses ilegal ke sistem elektronik, pencurian data, maupun penyebarluasan informasi yang merugikan. Pemahaman yang komprehensif terhadap unsur-unsur ini sangat penting bagi aparat penegak hukum dalam memproses kasus kejahatan siber, untuk mencegah terjadinya kekeliruan dalam penerapan hukum yang berpotensi merugikan para pihak yang terlibat. Eddy O.S. Hiariej menegaskan bahwa kesengajaan merupakan salah satu jenis kesalahan yang menjadi bagian dari unsur subjektif, di mana tingkat keseriusan hukuman potensial bergantung pada sifat perilaku buruk yang dilakukan.

Kasus Bjorka juga mengangkat isu penting mengenai hak korban untuk mendapatkan ganti kerugian atau pemulihan. UU PDP memberikan ruang bagi penjatuhan pidana tambahan berupa perampasan aset hasil kejahatan serta pembayaran ganti kerugian, sehingga korban berhak mengajukan restitusi agar dapat memperoleh kompensasi sejalan dengan proses penegakan hukum pidana. Mekanisme ini memberikan perlindungan yang lebih komprehensif bagi korban kejahatan siber, namun implementasinya masih memerlukan koordinasi yang lebih baik antara lembaga penegak hukum dan otoritas perlindungan data pribadi. Pasal 69 UU PDP mengatur kemungkinan penjatuhan pidana tambahan berupa perampasan aset yang diperoleh dari tindak pidana serta kewajiban membayar ganti kerugian, sehingga korban dapat mengajukan restitusi untuk mendapatkan pemulihan.

Berdasarkan latar belakang permasalahan yang telah dijelaskan sebelumnya, maka dapat dirumuskan beberapa masalah pokok yang menjadi fokus dalam penelitian ini. Pertama, bagaimana bentuk tindak pidana cybercrime yang dilakukan oleh Bjorka dalam kasus peretasan dan penyalahgunaan data pribadi, termasuk modus operandi, jenis pelanggaran yang dilakukan, serta dampaknya terhadap keamanan data masyarakat dan pemerintah. Kedua, bagaimana penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam penegakan hukum terhadap kasus tersebut, khususnya dalam menilai efektivitas regulasi dan langkah aparat penegak hukum dalam menghadapi tindak kejahatan siber yang semakin kompleks di era digital.

METODE

Penelitian ini menggunakan metode yuridis normatif dengan mengkaji norma hukum yang mengatur tindak pidana cybercrime serta perlindungan data pribadi dalam sistem hukum Indonesia. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan kasus (case approach) dengan menelaah ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Informasi dan Transaksi Elektronik, serta kasus peretasan dan penyalahgunaan data pribadi oleh hacker Bjorka. Analisis dilakukan secara kualitatif-deskriptif untuk menjelaskan penerapan hukum terhadap tindak pidana cybercrime sekaligus mengevaluasi efektivitas

penegakan hukum dan perlindungan terhadap korban pelanggaran data pribadi di Indonesia.

HASIL DAN PEMBAHASAN

Bentuk Tindak Pidana Cybercrime yang Dilakukan oleh Bjorka dalam Kasus Peretasan dan Penyalahgunaan Data Pribadi

Penangkapan Bjorka pada 23 September 2025 di Minahasa, Sulawesi Utara, menandai berakhirnya salah satu kasus kejahatan siber paling masif dalam sejarah Indonesia. Bjorka, seorang peretas yang telah menjadi sorotan publik sejak pertengahan 2022, dikenal karena serangkaian aksi peretasan dan kebocoran data pribadi yang melibatkan jutaan warga negara Indonesia, termasuk data dari berbagai instansi pemerintah dan lembaga strategis. Kasus ini tidak hanya menimbulkan keresahan publik yang luar biasa, tetapi juga mengekspos kerentanan sistem keamanan siber nasional yang mendesak untuk diperbaiki. Pengenaan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dengan ancaman pidana maksimal 12 tahun penjara dan denda hingga Rp12 miliar menunjukkan keseriusan negara dalam menangani kejahatan siber yang mengancam kedaulatan data dan privasi warga negara.

Tindak pidana pertama yang dilakukan Bjorka adalah akses ilegal ke sistem elektronik, yang merupakan inti dari seluruh rangkaian kejahatannya. Bjorka diduga melakukan penetrasi tidak sah ke berbagai basis data pemerintah dan swasta, termasuk sistem Direktorat Jenderal Imigrasi, Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, dan berbagai instansi lainnya. Modus operandi yang digunakan kemungkinan melibatkan teknik hacking canggih seperti SQL injection, phishing, atau eksploitasi kerentanan keamanan (vulnerability exploitation) pada sistem yang ditargetkan. Tindakan tersebut telah secara tegas ditentukan dalam Pasal 46 ayat (1) UU ITE, yang menyatakan bahwa setiap orang yang dengan sengaja serta tanpa hak atau secara melanggar hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 30 ayat (1) yaitu melakukan akses terhadap komputer dan/atau sistem elektronik milik orang lain dengan metode apa pun dapat dijatuhi hukuman pidana. Kritik yang muncul adalah bahwa meskipun undang-undang ini telah ada, implementasi sistem keamanan siber di Indonesia masih sangat lemah, sehingga memudahkan peretas seperti Bjorka untuk melancarkan aksinya tanpa hambatan berarti selama bertahun-tahun.

Setelah berhasil mengakses sistem elektronik, Bjorka kemudian melakukan pencurian data dalam skala masif yang mencakup informasi pribadi jutaan warga negara Indonesia. Data yang dicuri meliputi Nomor Induk Kependudukan (NIK), informasi paspor, data kesehatan dari BPJS, hingga data registrasi kartu SIM yang sangat sensitif. Perbuatan pencurian data ini dikategorikan sebagai tindak pidana berdasarkan Pasal 32 ayat (1) UU ITE melarang setiap orang untuk dengan sengaja dan tanpa hak atau secara melawan hukum melakukan tindakan apa pun yang berupa mengubah, menambah, mengurangi, mentransmisikan, merusak, menghapus, memindahkan, atau menyembunyikan informasi elektronik dan/atau dokumen elektronik milik pihak lain maupun milik publik. Pencurian data dalam konteks ini bukan sekadar perbuatan kriminal biasa, melainkan adalah salah satu bentuk pelanggaran terhadap hak asasi manusia terkait hak atas privasi sebagaimana dijamin dalam UUD 1945 Pasal 28G ayat (1), sehingga dampaknya melampaui kerugian material dan menciptakan ancaman jangka panjang terhadap keamanan personal korban.

Tindakan Bjorka tidak berhenti pada pencurian data, tetapi berlanjut dengan penyebarluasan data pribadi tersebut melalui berbagai platform internet, termasuk forum-forum dark web dan media sosial. Bjorka secara terbuka membagikan sampel data curian sebagai bentuk "pembuktian" atas keberhasilannya meretas sistem-sistem Indonesia, bahkan menawarkan data tersebut untuk dijual kepada pihak-pihak yang berkepentingan. Perbuatan ini secara eksplisit melanggar Pasal 26 UU ITE tentang perlindungan data pribadi, yang kemudian diperkuat dengan ketentuan dalam UU PDP. Penyebarluasan data ini menimbulkan efek domino yang sangat berbahaya: korban menjadi rentan terhadap berbagai bentuk kejahatan lanjutan seperti pencurian identitas (identity theft), penipuan (fraud), pemerasan, hingga ancaman keamanan fisik. Dari perspektif kritis, kasus ini mengungkapkan kegagalan sistemik dalam penegakan hukum perlindungan data di Indonesia, di mana sanksi yang ada belum memberikan efek jera yang memadai, dan mekanisme perlindungan preventif masih sangat terbatas.

Dimensi lain dari kejahatan Bjorka adalah upaya pemerasan dan intimidasi yang dilakukannya terhadap pemerintah Indonesia. Bjorka tidak hanya membocorkan data, tetapi juga melakukan tindakan yang dapat dikategorikan sebagai cyber extortion dengan mengancam akan terus membocorkan data lebih banyak jika tuntutannya tidak dipenuhi, serta melontarkan berbagai pernyataan provokatif yang merendahkan kapabilitas keamanan siber Indonesia. Tindakan ini dapat dijerat dengan Pasal 29 UU ITE mengatur mengenai ancaman kekerasan atau tindakan menakut-nakuti yang ditujukan kepada seseorang, meskipun dalam kasus ini sasaran utamanya adalah lembaga negara. Lebih jauh lagi, perbuatan Bjorka juga mengandung unsur cyber terrorism karena menimbulkan rasa takut massal dan mengancam stabilitas keamanan nasional. Argumentasi yang perlu dikemukakan adalah bahwa kejahatan siber seperti ini tidak dapat lagi dipandang sebagai kejahatan individu biasa, melainkan sebagai ancaman keamanan nasional yang memerlukan respons terintegrasi dari berbagai lembaga negara, termasuk penguatan kapasitas cyber defense dan intelligence Indonesia.

Aksi Bjorka juga menimbulkan gangguan signifikan terhadap operasional sistem elektronik berbagai instansi yang diretas, meskipun tidak ada laporan tentang kerusakan permanen pada sistem tersebut. Gangguan ini mencakup keharusan melakukan investigasi forensik digital, pemulihan sistem, peningkatan protokol keamanan darurat, dan upaya mitigasi dampak kebocoran data yang memerlukan sumber daya besar dan mengganggu pelayanan publik. Tindakan tersebut dapat digolongkan sebagai bentuk pelanggaran terhadap Pasal 33 UU ITE mengatur mengenai perbuatan yang dilakukan dengan sengaja dan tanpa hak atau secara melawan hukum yang menyebabkan terganggunya sistem elektronik dan/atau membuat sistem tersebut tidak berfungsi sebagaimana mestinya. Kritik yang perlu diajukan adalah bahwa pemerintah dan lembaga-lembaga yang menjadi korban seharusnya juga memikul tanggung jawab atas kelalaian dalam mengamankan data publik yang dipercayakan kepada mereka, sehingga penanganan kasus ini tidak boleh hanya fokus pada penghukuman pelaku tetapi juga pada reformasi tata kelola keamanan siber nasional.

Kasus Bjorka merepresentasikan kompleksitas kejahatan siber modern yang melibatkan multiple layers of criminality, mulai dari akses ilegal, pencurian data, penyebarluasan informasi pribadi, pemerasan, hingga gangguan terhadap kepentingan umum. Pengenaan UU ITE dengan ancaman pidana maksimal 12 tahun penjara dan denda Rp12 miliar menunjukkan bahwa hukum Indonesia telah mengantisipasi keseriusan kejahatan siber, namun efektivitas penegakan hukum ini sangat bergantung pada kemampuan aparat dalam melakukan investigasi digital dan menghadirkan bukti-bukti forensik yang kuat di pengadilan. Secara kritis, kasus ini seharusnya menjadi momentum bagi Indonesia untuk melakukan reformasi menyeluruh dalam sistem keamanan siber nasional, termasuk peningkatan investasi pada infrastruktur keamanan, capacity building bagi aparat penegak hukum, harmonisasi regulasi perlindungan data, dan pembangunan kesadaran literasi digital masyarakat. Tanpa langkah-langkah komprehensif tersebut, penangkapan Bjorka hanya akan menjadi kemenangan simbolis tanpa dampak preventif terhadap ancaman kejahatan siber di masa depan.

Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Penegakan Hukum terhadap Kasus Bjorka

Penanganan kasus Bjorka menghadirkan kompleksitas yuridis yang unik karena melibatkan penerapan dua instrumen hukum utama secara bersamaan, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE lebih menekankan pada aspek teknis kejahatan siber seperti akses ilegal, interferensi sistem, dan penyalahgunaan teknologi informasi, sementara UU PDP secara spesifik mengatur tentang perlindungan hak privasi individu atas data pribadinya. Dalam konteks kasus Bjorka, penerapan kedua undang-undang ini secara kumulatif memberikan landasan hukum yang komprehensif untuk menjerat pelaku dengan berbagai pasal yang relevan, mulai dari tindakan peretasan sistem hingga pencurian dan penyebarluasan data pribadi jutaan warga negara. Namun, penerapan kerangka hukum ganda ini juga menimbulkan pertanyaan kritis mengenai potensi tumpang tindih pengaturan dan

bagaimana aparat penegak hukum harus mengonstruksi dakwaan yang tepat untuk menghindari gugurnya dakwaan karena obscuur libel atau dakwaan yang tidak jelas.

Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan terbaru dari UU ITE memberikan instrumen hukum yang kuat untuk menjerat Bjorka atas tindakan peretasan dan akses ilegal yang dilakukannya. Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE secara tegas melarang akses ke komputer dan/atau sistem elektronik milik orang lain tanpa hak, dengan ancaman pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600 juta. Dalam kasus Bjorka yang melibatkan penetrasi ke multiple systems seperti basis data Direktorat Jenderal Imigrasi, BPJS Kesehatan, dan sistem registrasi SIM, penerapan pasal ini dapat dilakukan secara berlapis karena setiap akses ilegal ke sistem yang berbeda merupakan tindak pidana tersendiri. Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE yang mengatur tentang pemindahan atau pentransferan informasi elektronik dengan ancaman pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp2 miliar, juga sangat relevan mengingat Bjorka tidak hanya mengakses tetapi juga mengekstraksi data dalam jumlah masif. Kritik yang perlu dikedepankan adalah ancaman pidana yang ada masih belum sebanding dengan dampak masif yang ditimbulkan, sehingga perlu ada diskursus mengenai pemberatan hukuman khususnya untuk kejahatan siber yang berdampak pada keamanan nasional.

UU PDP memberikan dimensi jaminan hukum yang lebih spesifik terhadap aspek pencurian dan penyalahgunaan data pribadi yang menjadi inti pelanggaran dalam kasus Bjorka. Pasal 65 ayat (1) UU PDP menegaskan bahwa setiap orang yang dengan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri, dipidana dengan pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp5 miliar. Pasal 67 ayat (1) UU PDP mengatur tentang tindak pidana pengungkapan data pribadi secara melawan hukum, dengan ancaman pidana penjara paling lama 4 tahun dan/atau pidana denda paling banyak Rp4 miliar, yang sangat relevan dengan perbuatan Bjorka yang menyebarluaskan data curian melalui dark web dan media sosial. Tetapi, penerapan UU PDP undang-undang ini baru disahkan pada tahun 2022 dan banyak ketentuan pelaksanaannya belum terbentuk, termasuk belum terbentuknya Lembaga Pelindungan Data Pribadi sebagai otoritas pengawas, sehingga efektivitas penerapan UU PDP masih menghadapi berbagai hambatan implementatif meskipun secara substansi memberikan perlindungan yang sangat dibutuhkan.

Penerapan UU ITE dan UU PDP dalam kasus Sanksi terhadap Bjorka tidak hanya mencakup hukuman pokok berupa pidana penjara dan denda, tetapi juga membuka peluang penjatuhan pidana tambahan yang memberikan efek jera lebih besar dan keadilan restoratif bagi korban. Pasal 69 Undang-Undang Perlindungan Data Pribadi menetapkan adanya pidana tambahan berupa: penyitaan keuntungan dan/atau kekayaan yang diperoleh dari tindak pidana; penyitaan aset yang digunakan untuk melakukan tindak pidana; serta kewajiban membayar ganti rugi kepada korban. UU ITE juga memuat ketentuan mengenai pidana tambahan berupa pengumuman putusan pengadilan sebagaimana tercantum dalam Pasal 52, yang bertujuan memberikan efek pencegahan umum (general deterrence). Hakim juga dapat memerintahkan pemusnahan data curian yang masih dikuasai terpidana atau pihak ketiga, serta pemblokiran akses terhadap konten atau platform yang digunakan untuk menyebarkan data curian. Kritik yang muncul adalah implementasi pidana tambahan di lapangan masih menghadapi kendala, terutama mekanisme eksekusi ganti kerugian kepada korban yang jumlahnya masif dan tersebar, serta kompleksitas melacak dan merampas aset hasil kejahatan yang telah dikonversi ke berbagai bentuk termasuk cryptocurrency.

Implementasi UU ITE dan UU PDP dalam penegakan hukum kasus Bjorka menghadapi berbagai hambatan yang bersifat struktural dan teknis yang memerlukan perhatian serius dari seluruh stakeholder, yaitu:

1. Kapasitas aparat penegak hukum dalam menangani kejahatan siber yang masih sangat terbatas baik dalam aspek jumlah maupun mutu, sehingga dibutuhkan investasi serius dalam capacity building melalui pelatihan intensif, sertifikasi internasional, dan pengadaan peralatan forensik digital yang memadai.
2. Koordinasi antara lembaga-lembaga penegak hukum yang masih belum berjalan secara efektifpadahal kejahatan siber bersifat lintas sektoral dan memerlukan

kolaborasi antara polri, kejaksaan, bssn, bin, dan lembaga terkait lainnya, sehingga diperlukan pembentukan task force khusus dengan kewenangan dan mekanisme kerja yang jelas.

3. Aspek kerja sama internasional dalam penanganan kejahatan siber yang seringkali melibatkan yurisdiksi lintas negara, dimana indonesia masih menghadapi berbagai hambatan legal dan birokratis dalam mutual legal assistance dan ekstradisi dengan negara-negara lain.
4. Belum operasionalnya lembaga pelindungan data pribadi yang seharusnya menjadi garda terdepan dalam pengawasan dan penegakan hukum perlindungan data, yang menyebabkan banyak kasus pelanggaran data pribadi tidak dapat ditangani secara optimal.

Penerapan UU ITE dan UU PDP dalam kasus Bjorka memberikan pembelajaran berharga mengenai kekuatan dan kelemahan kerangka hukum perlindungan data dan penegakan hukum kejahatan siber di Indonesia yang memerlukan evaluasi komprehensif untuk penyempurnaan di masa mendatang. Aspek positif yang dapat dicatat adalah kedua undang-undang ini telah memberikan landasan hukum yang cukup komprehensif, memberikan pengakuan terhadap alat bukti elektronik, serta mengakomodasi kepentingan korban melalui mekanisme ganti kerugian dan restitusi. Namun terdapat kelemahan fundamental, yaitu:

1. ancaman pidana masih belum sebanding dengan dampak masif yang ditimbulkan;
2. implementasi UU PDP terhambat karena belum terbentuknya seluruh peraturan pelaksana;
3. masih terbatasnya kapasitas aparat dalam menangani bukti digital.

Penerapan UU PDP dan UU ITE dalam penegakan hukum terhadap kasus Bjorka menandai langkah penting dalam penguatan sistem hukum nasional di bidang keamanan siber dan perlindungan data pribadi. Kedua instrumen hukum ini berperan saling melengkapi: UU ITE menjadi dasar untuk menindak perbuatan teknis seperti peretasan, akses ilegal, dan manipulasi sistem elektronik, sementara UU PDP memperluas perlindungan terhadap hak privasi warga negara melalui pengaturan yang lebih rinci mengenai pengumpulan, penggunaan, dan penyebarluasan data pribadi. Sinergi antara keduanya mencerminkan upaya negara untuk menghadirkan perlindungan hukum yang menyeluruh dan adaptif terhadap dinamika kejahatan digital modern. Namun, efektivitas penerapannya masih menuntut penguatan kelembagaan, harmonisasi regulasi, serta peningkatan kapasitas aparat penegak hukum agar implementasi kedua undang-undang ini tidak hanya bersifat represif, tetapi juga mampu mewujudkan keadilan, keamanan digital, dan perlindungan hak fundamental warga negara secara berkelanjutan.

SIMPULAN

Kasus Bjorka mencerminkan bentuk kejahatan siber yang kompleks dan berlapis, mencakup akses ilegal, pencurian, serta penyebarluasan data pribadi yang menimbulkan dampak serius terhadap keamanan nasional dan hak privasi warga negara. Melalui penerapan berbagai pasal dalam UU ITE dan UU PDP, negara berupaya menegakkan hukum secara tegas terhadap pelaku, sekaligus memperlihatkan bahwa kejahatan siber tidak lagi sekadar pelanggaran teknis, melainkan ancaman terhadap kedaulatan digital Indonesia. Namun demikian, kasus ini juga menyoroti lemahnya sistem keamanan siber dan masih terbatasnya kapasitas penegakan hukum di Indonesia. Oleh karena itu, penyelesaian kasus Bjorka harus menjadi momentum penting untuk memperkuat kebijakan perlindungan data, memperbaiki tata kelola keamanan siber nasional, serta meningkatkan literasi digital masyarakat agar kejadian serupa tidak terulang di masa mendatang.

Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam penegakan hukum terhadap kasus Bjorka menunjukkan bahwa Indonesia telah memiliki dasar hukum yang cukup kuat dalam menghadapi kejahatan siber dan pelanggaran data pribadi. Kedua regulasi tersebut membentuk sinergi antara aspek teknis kejahatan digital dan perlindungan hak privasi masyarakat, sehingga mampu memberikan payung hukum yang komprehensif bagi negara

dalam menindak pelaku dan melindungi korban. Namun demikian, efektivitas implementasinya masih terkendala oleh keterbatasan kapasitas aparat penegak hukum, koordinasi lintas lembaga yang belum optimal, serta belum terbentuknya lembaga pengawas pelindungan data pribadi. Oleh karena itu, diperlukan langkah strategis berupa peningkatan kemampuan sumber daya manusia, harmonisasi kebijakan, dan percepatan pembentukan lembaga pengawas agar penerapan kedua undang-undang ini dapat berjalan efektif, menjamin kepastian hukum, dan memperkuat keamanan siber nasional di masa mendatang.

SARAN

Berdasarkan uraian dan analisis di atas, terdapat beberapa saran yang dapat dijadikan acuan untuk memperkuat penegakan hukum dan perlindungan data pribadi di Indonesia, yaitu:

1. Pemerintah perlu mempercepat pembentukan Lembaga Pelindungan Data Pribadi (LPDP) serta menyusun peraturan pelaksana dari Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Langkah ini penting agar mekanisme pengawasan, penegakan hukum, dan pemberian ganti kerugian kepada korban pelanggaran data pribadi dapat berjalan secara efektif dan terkoordinasi. Tanpa kehadiran lembaga pengawas yang berfungsi optimal, penerapan UU PDP berisiko menjadi tidak maksimal dan hanya bersifat simbolis tanpa dampak nyata bagi perlindungan hak privasi warga negara.
2. Diperlukan peningkatan kapasitas aparat penegak hukum dalam bidang forensik digital, keamanan siber, dan pemahaman regulasi teknologi informasi. Penguatan ini harus dilakukan melalui pelatihan teknis berkelanjutan, kerja sama dengan lembaga internasional, serta investasi pada infrastruktur pendukung penegakan hukum siber. Dengan demikian, aparat penegak hukum mampu melakukan investigasi yang akurat, efektif, dan berbasis bukti digital yang kuat, sehingga penegakan hukum terhadap kejahatan siber seperti kasus Bjorka dapat memberikan efek jera dan memperkuat kepercayaan publik terhadap sistem hukum nasional.

DAFTAR PUSTAKA

Agus Raharjo, Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi (Bandung: PT Citra Aditya Bakti, 2002)

Budi Suhariyanto, Tindak Pidana Teknologi Informasi (Cybercrime) : Urgensi Pengaturan Dan Celah Hukumnya (Jakarta: Raja Grafindo Persada, 2013)

Danrivanto Budhijanto, Hukum Telekomunikasi, Penyiaran, Dan Teknologi Informasi: Regulasi Dan Konvergensi (Bandung: Refika Aditama, 2010)

———, Revolusi Cyberlaw Indonesia : Pembaruan Dan Revisi UU ITE 2016 (Bandung: Refika Aditama, 2017)

Dikdik M. Arief Mansur, Cyber Law: Aspek Hukum Teknologi Informasi (Bandung: Refika Aditama, 2005)

Edmon Makarim, Kompilasi Hukum Telematika (Jakarta: University Press, 2003)

———, Tamggung Jawab Hukum Penyelenggara Sistem Elektronik (Jakarta: Raja Grafindo Persada, 2010)

Hiarej, Eddy O.S., Prinsip-Prinsip Hukum Pidana (Yogyakarta: Cahaya Atma Pustaka, 2016)

Hosnah, Asmak Ul, Herli Antoni, and Ravi Yofany, 'Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law', International Journal of Multicultural and Multireligious Understanding, 11, 2023, 362–72

Indonesia, Undang-Undang Tentang Informasi Dan Transaksi Elektronik

Josua Sitompul, Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana (Jakarta: Tatanusa, 2012)

M Zaki Rizaldi, Rizki Dwi Putra, Asmak Ul Hosnah, 'Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data', Jurnal Ilmu Hukum Dan Humaniora, 6.2 (2023), 234–49

Maskun, Kejahatan Siber (Cyber Crime): Suatu Pengantar (Jakarta: Kencana Prenada Media Group, 2013)

Nadya Putri í, Annisa, 'Upaya Hukum Dalam Strategi Perlindungan Data Pada Penggunaan Internet Studi Kasus : Hacker Bjorka', Jurnal Hukum Dan Pembangunan Ekonomi, 12.1

(2024), 2024

Pusiknas Polri, 'Hacker Berusia 22 Tahun Ditangkap Setelah Retas Data Bank' <https://pusiknas.polri.go.id/detail_artikel/hacker_berusia_22_tahun_ditangkap_setelah_retas_data_bank>

———, 'Statistik Kriminal Periode 1 Januari 2025 s.d 26 Oktober 2025' <https://pusiknas.polri.go.id/data_kejahatan>

Wahyudi Djafar, Perlindungan Hak Atas Privasi Di Internet: Beberapa Penjelasan Kunci (Jakarta: ELSAM, 2014)

Wijaya, Johan, Aji Titin Roswitha Nursanthy, and Muhammad Arganata Thamrin, 'Perlindungan Terhadap Data Pribadi Dalam Berselancar Di Dunia Maya', The Juris, 8.2 (2024), 638–44 <https://doi.org/10.56301/juris.v8i2.1477>

Wuwungan, Meyse Stevely Sisilia, Cornelis Dj. Massie, and Josepus Jullie Pinori, 'Perlindungan Hukum Terhadap Pemilik Data Pribadi Pengguna Teknologi Informasi Akibat Tindak Pidana Peretasan', Jurnal Lex Privatum, 13.4 (2024), 146–60