URGENSI PENGUATAN REGULASI PELINDUNGAN DATA DAN KEAMANAN SIBER DI INDONESIA TERHADAP ANCAMAN *HACKING* DALAM SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Christopher Kristian Darmawan; Ezra Sebastian; Frederick Leroy Notokusumo; Jeshua Resa Loprang
christopherkristian@gmail.com ; ezraeca99@gmail.com ; fickowang@gmail.com ; jrloprang@gmail.com
Afiliasi
Fakultas Hukum, Tangerang, Universitas Pelita Harapan

Abstract

The rapid advancement of information technology has introduced new challenges in cybercrime enforcement. The Bjorka case, involving data breaches and leaks of state secrets, highlights the weaknesses in Indonesia's cyber regulations. This study aims to analyze the limitations and effectiveness of Indonesia's Electronic Information and Transactions Law (UU ITE) and Personal Data Protection Law (UU PDP) in addressing cybercrime, comparing them with the cyber law framework in the United States. This research employs a normative juridical approach with a comparative analysis of both legal systems. The findings reveal that UU ITE lacks specific provisions on transnational cybercrime, cross-border jurisdiction mechanisms, and critical information infrastructure protection. In contrast, the United States has a more comprehensive legal framework, such as the Computer Fraud and Abuse Act (CFAA) and the CLOUD Act, which provide broader enforcement authority in handling similar cases. This study recommends the establishment of more specific cybercrime regulations, strengthening international cooperation, and enhancing law enforcement capabilities in cyber investigations. By implementing a more adaptive legal framework, Indonesia can effectively mitigate the growing threats of cybercrime thru Indonesia Cyber security and resilience law (RUU KKS)

Keywords: *Cybercrime, Bjorka, UU ITE, UU PDP , Indonesia Cyber Law, RUU KKS*

Abstrak

Kemajuan teknologi informasi yang pesat telah menimbulkan tantangan baru dalam penegakan kejahatan siber. Kasus Bjorka, yang melibatkan pembobolan data dan pembocoran rahasia negara, menyoroti kelemahan dalam peraturan siber di Indonesia. Penelitian ini bertujuan untuk menganalisis keterbatasan dan efektivitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam menangani kejahatan siber, serta membandingkannya dengan kerangka kerja hukum siber di Amerika Serikat. Penelitian ini menggunakan pendekatan normatif empiris dengan analisis komparatif terhadap kedua sistem hukum tersebut. Temuan menunjukkan bahwa UU ITE tidak memiliki ketentuan khusus mengenai kejahatan siber transnasional, mekanisme yurisdiksi lintas

negara, dan perlindungan infrastruktur informasi yang penting. Sebaliknya, Amerika Serikat memiliki kerangka hukum yang lebih komprehensif, seperti *Computer Fraud and Abuse Act* (CFAA) dan *CLOUD Act*, yang memberikan kewenangan penegakan hukum yang lebih luas dalam menangani kasus-kasus serupa. Studi ini merekomendasikan pembentukan peraturan kejahatan siber yang lebih spesifik, memperkuat kerja sama internasional, dan meningkatkan kemampuan penegakan hukum dalam investigasi siber. Dengan menerapkan kerangka hukum yang lebih adaptif, Indonesia dapat secara efektif mitigasi ancaman kejahatan siber yang terus meningkat melalui RUU Keamanan dan Ketahanan Siber (RUU KKS).

Kata kunci: kejahatan siber, Bjorka, UU ITE, UU PDP, Hukum Siber Indonesia, RUU KKS

A. PENDAHULUAN

Data Pribadi merupakan sejumlah data atau informasi pribadi yang dimiliki oleh hampir seluruh manusia di dunia. Merujuk pada Pasal 1 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), data pribadi merupakan 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 dapat diidentifikasi secara tersendiri atau digabungkan dengan informasi lain. Informasi tersebut bersifat privasi sehingga harus dipertanggungjawabkan penggunaanya oleh seluruh pihak yang bersangkutan, baik pihak pemilik data maupun pengendali ataupun prosesor. Bentuk pertanggungjawaban ini dapat diwujudkan melalui perlindungan terhadap data pribadi tersebut. Perlindungan data pribadi merupakan salah satu bentuk perlindungan hak asasi manusia, sebagaimana tercantum dalam Pasal 28G ayat (1) Undang-Undang Dasar 1945 (UUD 1945), yang berbunyi *"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".* Perlindungan data pribadi merupakan tanggung jawab bagi seluruh pihak, baik pihak subjek data pribadi sebagai pemilik data maupun pihak pengendali atau prosesor data. Pemerintah dalam hal ini merupakan salah pihak yang memiliki peran utama dalam penyelenggaraan perlindungan data pribadi. Dengan demikian, sudah seyogyanya bangsa Indonesia memberikan perlindungan data pribadi yang optimal bagi seluruh masyarakatnya. Perkembangan kejahatan dengan menggunakan teknologi internet juga semakin beragam seiring dengan perkembangan teknologi itu sendiri, mulai dari *internet abuse, hacking, carding,* dan sebagainya.

Akan tetapi, pada kenyataanya Indonesia masih menjadi negara ke 3 dengan paling banyak kebocoran data terbanyak di Dunia.[1] Peretasan sendiri

[1] Databoks.katadata.co.id, "Indonesia Masuk 3 Besar Negara Dengan Kasus Kebocoran Data Terbanyak Dunia: Databoks," *Pusat Data Ekonomi Dan Bisnis Indonesia*, accessed March 15, 2025,

sudah dirumuskan di dalam *International Information Industry Congress* (IIC) tahun 2000 di Kanada telah dirumuskan mengenai kewaspadaan perkembangan *cyber crime* yang dapat merusak sistem dan data teknologi negara dan perusahaan.[2] *Hacking* juga merupakan tindakan kriminal yang dapat menimbulkan kepanikan atau kekacauan massal di tengah masyarakat.

Hacking dapat ditujukan kepada semua *website* dan semua jenis aktivitas digital. Salah satunya adalah Sistem Pemerintahan Berbasis Elektronik. SPBE sendiri adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.[3] Perencanaan SPBE ini selaras dengan Peraturan Presiden (PERPRES) Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. Namun, dalam penerapan SPBE sendiri terdapat beberapa kelemahan dari banyaknya aplikasi dan sikap lembaga pemerintah yang mempertahankan keberadaan aplikasi dan biaya yang besar yang menyebabkan kerawanan dalam korupsi dan keamanan.[4]

Kurangnya standar keamanan terhadap sistem elektronik dan sertifikasi keamanan. Menurut Perpres 82/2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional Indonesia memiliki berbagai program melalui layanan Satu Data Indonesia dalam melayani dan mendukung penyelenggaraan Pertukaran data dan tata kelola data dalam SPBE.

Hal ini membuat resiko dan terjadi *hacking* yang dilakukan oleh bjorka dari Badan Intelijen Negara, Komisi Pemilihan Umum, Presiden Jokowi,dll. berupa data nama lengkap, nomor KTP, nomor Kartu Keluarga (KK), nama orang tua, alamat rumah, tempat dan tanggal lahir, status agama, riwayat pendidikan, dan sebagainya. [5]

Sehingga, dengan ini Tim peneliti mengambil 2 (dua) rumusan masalah yaitu (1) Bagaimana pengaturan normatif terhadap kasus *hacking* bjorka terhadap Data Pribadi dan (2) Bagaimana mengoptimalisasikan peraturan perundang-undangan di Indonesia sebagai upaya preventif peretasan atau *hacking* di Indonesia berdasarkan studi komparasi dengan Amerika Serikat. untuk mengetahui *gap* regulasi hukum *cyber* di Indonesia serta menganalisis kekurangan serta memberikan saran kepada pemerintah dalam upaya preventif terhadap

https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/3f6a7dc0c5d0b7e/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia

[2] Willa Wahyuni, "Jerat Hukum Peretasan Oleh Hacker," *Hukumonline.Com*, accessed March 15, 2025, https://www.hukumonline.com/berita/a/jerat-hukum-peretasan-oleh-hacker-lt631ec0ed9e52c

[3] Pasal 1 Butir 1 PERPRES No. 95 Tahun 2018. (n.d.). Database Peraturan | JDIH BPK. https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018

[4] Antonius Galih Prasetyo, "Prasyarat Keberhasilan Dan Nilai Tambah 'Super App,'" *Kompas.Id*, July 31, 2022, accessed March 15, 2025, https://www.kompas.id/baca/opini/2022/07/28/prasyarat-keberhasilan-dan-nilai-tambah-super-app

[5] Artika Rachmi Farmita and Inge Klara Safitri, "Sosok Bjorka, Peretas Yang Mengacak-ACAK Sistem Data Indonesia," *Tempo.Co*, September 12, 2022, accessed March 15, 2025, https://www.tempo.co/infografik/infografik/sosok-bjorka-peretas-yang-mengacak-acak-sistem-data-indonesia-875

hacking melalui RUU Ketahanan dan Keamanan Siber (RUU KKS) yang menjadi payung hukum yang lebih komprehensif dalam mengatur keamanan di dunia siber serta mengevaluasi efektivitas regulasi di Indonesia dalam melindungi data pribadi.

B. METODE PENELITIAN

Penelitian ini menggunakan metode normatif-empiris yaitu penggabungan antara pendekatan hukum normatif dengan adanya penambahan berbagai unsur empiris. Pendekatan normatif dilakukan dengan mengkaji peraturan perundang-undangan terkait *cyber law*, hukum pidana, dan perlindungan data pribadi, sedangkan pendekatan empiris dilakukan dengan meneliti implementasi regulasi dalam praktik melalui studi kasus dan analisis putusan pengadilan. Penelitian hukum normatif- empiris mengenai implementasi ketentuan hukum normatif (undang-undang) dengan metode pendekatan perundang-undangan (*statute approach*) dan komparasi atau perbandingan hukum untuk menganalisis kebijakan hacking yang dilakukan Bjorka, serta kebijakan yang diperlukan untuk mencegah hal itu.

Instrumen penelitian yang digunakan meliputi dokumen hukum, seperti undang-undang, regulasi, putusan pengadilan, dan laporan terkait keamanan siber. Data yang diperoleh dianalisis menggunakan metode deskriptif-kualitatif, yaitu dengan mendeskripsikan serta menginterpretasikan data berdasarkan kajian normatif dan empiris. Analisis normatif dilakukan dengan meneliti isi peraturan dan perbandingannya dengan praktik hukum di negara lain, sedangkan analisis empiris dilakukan dengan menelaah putusan pengadilan dan studi kasus terkait *hacking* untuk mengidentifikasi *gap* regulasi dan tantangan dalam implementasi hukum. Dalam penelitian ini, prinsip etika penelitian tetap dijaga dengan memperhatikan keabsahan dan kredibilitas sumber hukum yang digunakan, serta mempertimbangkan perkembangan terbaru dalam hukum siber dan teknologi digital sebagai faktor penting dalam penyusunan rekomendasi kebijakan.

Pendekatan ini mengkaji norma-norma yang ada dalam peraturan hukum terkait *cyber law*, hukum pidana, dan putusan pengadilan di Indonesia serta mengidentifikasi *gap* regulasi yang perlu diperbaiki, serta pendekatan komparatif dalam menganalisis peraturan perundang-undangan dan strategi di negara lain. Penelitian ini dilakukan selama 3 bulan dimulai dari Januari 2025 hingga Maret 2025, dengan lokasi penelitian mencakup studi literatur dan analisis dokumen hukum yang relevan. Sasaran penelitian ini adalah analisis implementasi regulasi terkait *hacking* dan keamanan siber di Indonesia, dengan fokus pada kasus Bjorka serta kebijakan yang diperlukan untuk mencegah kejahatan serupa di masa depan. Subjek penelitian meliputi regulasi hukum yang berlaku, seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi

Elektronik *jo*. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-undang Nomor 1 Tahun 2023 Kitab Undang-Undang Hukum Pidana (KUHP Baru), dan UU PDP, serta putusan pengadilan terkait *hacking* di Indonesia, termasuk perbandingan regulasi *cyber law* dari negara Amerika Serikat

C. PEMBAHASAN DAN HASIL

Pengaturan Normatif terhadap Perlindungan Data Pribadi dan Implikasinya dengan Peretasan Hacking oleh Bjorka

A. Latar Belakang dan Pengaturan Normatif Kasus Bjorka

Kasus peretasan atau *hacking* yang sempat menggemparkan jagat raya Indonesia terjadi pada tahun 2022 lalu. Pada bulan Agustus tahun 2022, sekelompok *hacker* atau peretas bernama Bjorka melakukan aksi penyerangan *cyber* terhadap berbagai infrastruktur digital negara Indonesia. Kelompok *hacker* ini meretas 26 juta data yang diklaim sebagai data pelanggan Indihome, kemudian membagikan atau menjual data-data tersebut di *Platform* Breached Forums. Data tersebut terdiri dari data riwayat pencarian pelanggan, nomor Kartu Tanda Penduduk (KTP) pelanggan, nama pelanggan, alamat email, dan lain-lain. [6]

Aksi sekelompok *hacker* ini tidak berhenti disitu saja. Mereka juga melakukan penyerangan atau *doxing* terhadap para pejabat pemerintahan Indonesia. Salah satu pejabat pemerintahan yang terkena *doxing* adalah Menteri Komunikasi dan Digital Indonesia, Bapak Johnny G. Plate, dimana data-data pribadinya disebarluaskan oleh Bjorka.[7] Selain dari itu, Bjorka mengklaim telah menyebarluaskan data pribadi milik Presiden Joko Widodo yang disimpan dalam beberapa dokumen di suatu *file* terkompres dengan besar 40 MB. *File* tersebut diberi judul "Permohonan Dukungan Sarana dan Prasarana", "Surat Rahasia Kepada Presiden", dan lain-lain. Walaupun begitu, klaim tentang tersebarnya data pribadi presiden sudah dibantah oleh Kepala Sekretariat Presiden (Kasetpres), Heru Budi Hartono. Ia mengatakan bahwa tidak ada dokumen surat milik Presiden yang telah disebarluaskan. [8]

Terakhir, kelompok *hacker* ini juga mengklaim telah menyebarkan data-data sensitif yang berasal dari SPBE berbagai instansi pemerintahan, seperti data Komisi Pemilihan Umum (KPU), Direktorat Jenderal Pajak (DJP), dan sebagainya. Sebanyak enam juta data dari DJP dijual di *platform*

[6] Zulfikar Hardiansyah, "APA ITU Breached Forums Yang Terlibat 4 Kasus Kebocoran Data Di Indonesia Sebulan Terakhir?," *KOMPAS.Com*, September 7, 2022, accessed March 15, 2025, https://tekno.kompas.com/read/2022/09/07/16150067/apa-itu-breached-forums-yang-terlibat-4-kasus-kebocoran-data-di-indonesia

[7] Zulfikar Hardiansyah, "Rentetan Aksi Hacker Bjorka Dalam Kasus Kebocoran Data Di Indonesia Sebulan Terakhir Halaman All," *KOMPAS.Com*, September 12, 2022, accessed March 15, 2025, https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all

[8] Desy Setyowati, "Daftar Data Diambil Hacker Bjorka Dan Bahayanya Bagi Warga Indonesia," *Teknologi Katadata.Co.Id*, accessed March 15, 2025, https://katadata.co.id/digital/teknologi/631ec2eb7a23a/daftar-data-diambil-hacker-bjorka-dan-bahayanya-bagi-warga-indonesia

Breached Forums dengan harga US$ 10 ribu atau Rp 150 juta. Mereka diduga menyertakan 10 ribu sampel yang didalamnya berisi rincian data pajak yang disebarluaskan. Data-data pajak yang disebarluaskan ini meliputi data-data pribadi dari wajib pajak, seperti nama wajib pajak, Nomor Induk Kependudukan, Nomor Pokok Wajib Pajak, dan lain-lain.[9]

Dalam merespons aksi *hacking* yang dilakukan oleh Bjorka, sejatinya Indonesia telah mempunyai payung hukum yang jelas dalam menghadapi perkara seperti ini. UU PDP, UU ITE, KUHP Baru, dan berbagai peraturan pelaksana, sejatinya telah mengatur tentang kejahatan peretasan atau *hacking*. Aksi peretasan yang dilakukan oleh Bjorka telah diatur ketentuannya dalam berbagai peraturan perundang-undangan tersebut. Secara garis besar, UU PDP sudah mengatur tentang perlindungan data pribadi orang perseorangan di Indonesia. Melalui UU PDP, para peretas atau *hacker* dapat dijatuhi sanksi berupa pidana penjara dan denda yang tidak sedikit. Hal ini diatur dalam Pasal 65 dan 67 UU PDP. Selain melalui UU PDP, UU ITE dan KUHP Baru juga telah memberikan ketentuan yang cukup untuk memberikan rasa jera terhadap para peretas atau *hacker*. UU ITE sejatinya telah mengatur tentang berbagai kejahatan digitalisasi, salah satunya tentang peretasan atau *hacking*. Hal ini diatur dalam Pasal 30 ayat (3), Pasal 32 ayat (1), Pasal 46 ayat (2), Pasal 48 ayat(1), dan Pasal 52 ayat (3) UU ITE. Aksi peretasan yang dilakukan oleh Bjorka juga termasuk delik pidana sehingga diatur pula ketentuannya dalam KUHP Baru. KUHP terbaru telah mengatur tindak pidana yang berkaitan dengan dunia digital, salah satunya *hacking* atau peretasan. Hal ini diatur dalam Pasal 333 huruf c dan d, Pasal 334 huruf a, dan Pasal 335 KUHP Baru. Dengan demikian, sejatinya pemerintah Indonesia telah memiliki landasan hukum yang jelas dalam mengatur tindakan peretasan atau *hacking* di Indonesia, terutama dalam hal pemberian sanksi atau denda. Akan tetapi, yang harus diperhatikan adalah apakah ketentuan tersebut sudah cukup untuk mencegah atau memitigasi peretasan atau *hacking* di Indonesia.

B. Analisis Pengaturan Normatif Terhadap Kasus Bjorka

Meninjau pada UU PDP, maka tindakan pengumpulan dan penjualan data pelanggan Indihome dan berbagai instansi pemerintahan yang dilakukan oleh Bjorka, melanggar Pasal 65 ayat (1) UU PDP, yang berbunyi "*setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi".* Pelanggaran yang dilakukan Bjorka terhadap ketentuan pasal tersebut dapat dijatuhi sanksi pidana berupa pidana penjara dan denda, sebagaimana dinyatakan dalam Pasal 67 ayat (1) UU PDP, yang berbunyi

[9] Melynda Dwi Puspita and Grace gandhi, "Nama Bjorka Disebut-Sebut Dalam Pembobolan 6 Juta NPWP, Ada Data Milik Jokowi, Gibran, Hingga Sri Mulyani," *Tempo*, September 19, 2024, accessed March 15, 2025, https://www.tempo.co/ekonomi/nama-bjorka-disebut-sebut-dalam-pembobolan-6-juta-npwp-ada-data-milik-jokowi-gibran-hingga-sri-mulyani--8048

"Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah)." Selain itu, tindakan *doxing* yang dilakukan oleh Bjorka terhadap Presiden dan pejabat-pejabat pemerintahan lainnya melanggar ketentuan Pasal 65 ayat (2) UU PDP, yang berbunyi *"setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya".* Konsekuensi terhadap tindakan *doxing* yang dilakukan oleh Bjorka dapat berupa pidana penjara dan/atau denda, sebagaimana dinyatakan dalam Pasal 67 ayat (2) UU PDP, yang berbunyi *"setiap orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah)."*

Selain melanggar ketentuan yang ada dalam UU PDP, Bjorka juga melanggar berbagai pasal atau ketentuan yang diatur dalam UU ITE dan KUHP Baru. Ditinjau dari UU ITE, maka tindakan Bjorka yang secara ilegal menerobos sistem pengamanan berbagai instansi swasta maupun pemerintah, dapat dikenakan Pasal 30 ayat (3) UU ITE, yang berbunyi *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."* Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi pidana berupa penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000,000,00 (delapan ratus juta rupiah), sebagaimana dinyatakan dalam Pasal 46 ayat (3), yang berbunyi *"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000,000,00 (delapan ratus juta rupiah)".* Konsekuensi atau sanksi yang harus diterima Bjorka akan lebih berat karena perbuatan ilegal yang dilakukannya ditujukan kepada pihak pemerintah dan badan strategis negara lainnya. Sehingga ancaman hukuman pidananya akan ditambah dua pertiga, sebagaimana dinyatakan dalam Pasal 52 ayat (3) UU ITE, yang berbunyi "*dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategik termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing pasal ditambah*

dua pertiga." Selain itu, tindakan Bjorka yang mengklaim telah menyimpan dokumen-dokumen atau data pribadi milik para pejabat pemerintahan dan Presiden Joko Widodo dapat melanggar Pasal 32 ayat (1) UU ITE, yang berbunyi "*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.* Pelanggaran terhadap pasal ini dapat dikenakan sanksi pidana berupa penjara paling lama 8 (delapan) dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah), sebagaimana dinyatakan dalam Pasal 48 ayat (1), yang berbunyi *"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah)."*[10]

Aksi *Hacking* atau peretasan yang dilakukan oleh Bjorka dapat dijerat dengan ketentuan-ketentuan hukum pidana dalam Undang-Undang No.1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Pembobolan dan perolehan data-data sensitif dari KPU dan DJP yang dilakukan Bjorka, dapat dikenakan sanksi berupa pidana penjara atau denda. Hal ini diatur dalam Pasal 335 KUHP Baru, yang berbunyi *"setiap orang yang tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik dengan cara apapun, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi, dipidana dengan pidana penjara paling lama 12 (duabelas) tahun atau pidana denda paling banyak kategori VII."* Selain itu, tindakan Bjorka yang membobol DJP sebagai lembaga perbankan, kemudian menjualnya di *platform* Breached Forums untuk kepentingan kepentingan pribadi, dapat dikenakan pidana penjara atau denda. Hal ini diatur dalam dalam Pasal 334 huruf a KUHP Baru, yang berbunyi *"dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling banyak kategori VI, setiap orang yang tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan yang dilindungi, dengan maksud menyalahgunakan, atau untuk mendapatkan keuntungan."*[11]

Berdasarkan penjabaran Pasal di atas, maka aksi peretasan atau *hacking* yang dilakukan Bjorka dapat dikenakan ketentuan pasal-pasal dalam

[10]Pasal 30 ayat (3), Pasal 32 ayat (1), Pasal 46 ayat (3), dan Pasal 52 ayat (3) UU No. 11 Tahun 2008. (n.d.). Database Peraturan | JDIH BPK. https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-2008

[11] Pasal 334 huruf a dan Pasal 335 UU No. 1 Tahun 2023. (n.d.). Database Peraturan | JDIH BPK. https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023

tiga peraturan perundang-undangan, yaitu UU PDP, UU ITE, dan KUHP Baru. Ketentuan yang dapat dikenakan kepada Bjorka, yaitu Pasal 65 ayat (1) dan (2) dan Pasal 67 ayat (1) dan (2) UU PDP, Pasal 30 ayat (3), Pasal 32 ayat (1), Pasal 46 ayat (3), dan Pasal 52 ayat (3) UU ITE, serta Pasal 334 huruf a dan Pasal 335 KUHP Baru.

C. Analisis Sistem Pemerintahan Berbasis Elektronik (SPBE) terhadap kasus Bjorka

Dalam membahas kasus peretasan yang dilakukan oleh Bjorka, Sistem Pemerintahan Berbasis Elektronik (SPBE) sudah sepatutnya menjadi salah satu aspek yang patut diperhatikan. Hal ini karena SPBE sendiri memiliki tujuan tata kelola pemerintahan, pelayanan publik, dan sistem pemerintahan berbasis elektronik di Indonesia.[12] Dengan demikian, implementasi SPBE memiliki peran penting dalam mencegah terjadinya tindakan peretasan data di Indonesia. Apabila ditinjau dalam beberapa tahun terakhir, SPBE sebenarnya telah menunjukan perkembangan yang cukup baik. Hal ini ditunjukan dari data evaluasi yang dirilis oleh Kementrian Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PANRB). Evaluasi ini dilaksanakan dengan mengukur tingkat kematangan (*maturity level*) penerapan SPBE pada instansi pusat dan pemerintah daerah yang direpresentasikan dalam bentuk nilai indeks. Berdasarkan data evaluasi tersebut, indeks SPBE Nasional mencapai predikat "baik" dengan angka indikator 3,12.[13] Angka ini sejatinya telah melampaui target nilai atau indeks yang dicantumkan dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN) Tahun 2020-2024.[14] Akan tetapi, meninjau pada maraknya kasus pembobolan atau peretasan data yang kian banyak terjadi di Indonesia selama beberapa tahun terakhir, tampaknya implementasi atau pelaksanaan SPBE di Indonesia masih harus ditingkatkan. Dalam hal ini, aspek atau prinsip keamanan SPBE menjadi hal yang patut diperhatikan oleh pemerintah.

Kasus peretasan yang dilakukan oleh Bjorka sudah selayaknya menjadi bahan evaluasi pemerintah dalam mengimplementasikan Sistem Pemerintahan Berbasis Elektronik (SPBE). Dalam melaksanakan aksi peterasannya, Bjorka berhasil membobol sistem keamanan data berbagai instansi pemerintahan dan swasta, kemudian memperoleh dan menjual data para pelanggan atau individu tertentu di *platform* Breached Forums. Hal ini menunjukan adanya

[12] Dss, "Sistem Pemerintahan Berbasis Elektronik (SPBE)," *Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi*, accessed March 15, 2025,. https://www.menpan.go.id/site/kelembagaan/sistem-pemerintahan-berbasis-elektronik-spbe-2

[13] Jane Kasia, "Indeks Spbe Nasional Meningkat, Menteri Rini: Penguatan Integrasi Pelayanan Publik Berbasis Digital," *Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi*, Januari 6, 2025 accessed March 15, 2025, https://www.menpan.go.id/site/berita-terkini/indeks-spbe-nasional-meningkat-menteri-rini-penguatan-integrasi-pelayanan-publik-berbasis-digital

[14] PERPRES No. 18 Tahun 2020. (n.d.). Database Peraturan | JDIH BPK. https://peraturan.bpk.go.id/Details/131386/perpres-no-18-tahun-2020

kelemahan dalam pengimplementasian prinsip-prinsip SPBE, yang didalamnya menyangkut Rencana Induk SPBE Nasional; Arsitektur SPBE; Peta Rencana SPBE; rencana dan anggaran SPBE; Proses Bisnis; data dan informasi; Infrastruktur SPBE; Aplikasi SPBE; Keamanan SPBE; dan Layanan SPBE. Dalam hal ini unsur Infrastruktur SPBE dan Keamanan SPBE merupakan hal-hal yang harus ditingkatkan oleh pemerintah.[15] Dengan demikian, untuk mencegah terjadinya kebobolan dalam sistem keamanan dari instansi pemerintahan dan juga memperkuat SPBE, alangkah baiknya Peraturan Presiden Nomor 95 Tahun 2018 Sistem Pemerintahan Berbasis Elektronik (Perpres SPBE 95/2018) diselaraskan dengan aspek atau isi UU PDP.

Perpres SPBE memiliki kelemahan signifikan dan dibutuhkan pengoptimalisasian lebih lanjut. Hal ini dapat dilihat ketika ada kejadian kebocoran data. Dalam hal ini, Perpres SPBE 95/2018 tidak menyebutkan langkah-langkah yang harus dilakukan ketika terjadi kebocoran data pribadi. Hal ini berbeda dengan Pasal 46 UU PDP yang menjelaskan bahwa kebocoran data pribadi wajib dilaporkan kepada pemilik data pribadi yang terkena dan lembaga yang terkait. Tujuan dari hal ini adalah untuk menunjukkan transparansi dari instansi pemerintah yang dimana juga merupakan basis dalam pertimbangan Perpres SPBE. Selain itu, Perpres SPBE tidak mengatur bentuk pertanggungjawaban atau akuntabilitas badan publik yang gagal atau lalai dalam mengelola keamanan data pribadi. Hal ini patut diperhatikan karena instansi swasta maupun pemerintah merupakan pihak bertanggung jawab dalam mencegah terjadinya kebocoran data. Dalam kasus Bjorka, tidak bisa dipungkiri bahwa instansi pemerintah gagal dalam mencegah kebocoran data tersebut. Dalam Pasal 57 UU PDP menjelaskan mengenai sanksi administratif karena pelanggaran atau kelalaian terhadap kewajiban dalam mengelola data. Dengan adanya sanksi yang diterapkan, maka harapannya instansi-instansi pemerintah bisa lebih serius dalam mengelola keamanan data pribadi.

Optimalisasi Pengaturan dan Pencegahan *Cyber Law* di Indonesia melalui Pengesahan RUU KKS dan Komparasi dengan Amerika Serikat

A. Optimalisasi Pengaturan Cyber Law dan Pencegahan Peretasan di Indonesia dan Amerika Serikat

Lemahnya pengawasan dan penerapan terhadap rumusan kebijakan yang ada dalam rumusan masalah pertama menunjukkan adanya celah regulasi dan ketidakefektifan mekanisme implementasi yang berlaku saat ini. Hal ini mengindikasikan bahwa pemerintah seharusnya tidak hanya mengandalkan peraturan normatif yang telah disusun sebelumnya, tetapi juga melakukan evaluasi secara menyeluruh terhadap efektivitas pengaturan yang ada. Salah satu cara yang dapat ditempuh adalah

[15] Pasal 2 ayat (1) PERPRES No. 95 Tahun 2018. (n.d.). Database Peraturan | JDIH BPK. https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018

dengan membandingkan dan belajar dari praktik terbaik di negara lain, seperti Amerika Serikat (USA), yang telah memiliki pengalaman lebih dalam mengatur isu terkait melalui kebijakan serupa.

Komparasi dengan Amerika Serikat menjadi relevan karena negara tersebut telah memiliki sistem hukum yang lebih matang dalam menangani berbagai isu kebijakan, termasuk dalam bidang keamanan, siber, dan hak asasi manusia. Dalam konteks kebijakan keamanan dan ketahanan, AS telah mengembangkan berbagai mekanisme yang memungkinkan koordinasi efektif antara lembaga pemerintah, penegak hukum, serta sektor swasta, sehingga kebijakan yang diterapkan lebih terintegrasi dan dapat dijalankan secara optimal.

Dengan melakukan perbandingan terhadap model regulasi AS, Indonesia dapat mengambil pelajaran mengenai keberhasilan serta kekurangan dalam penerapan kebijakan serupa, sehingga dapat mengadaptasi model yang sesuai dengan kondisi sosial, politik, dan hukum di Indonesia. Lebih jauh lagi, pendekatan komparatif ini juga dapat membantu dalam menyusun mekanisme pengawasan dan evaluasi yang lebih efektif agar regulasi yang disusun tidak hanya bersifat normatif, tetapi juga dapat diterapkan dengan mekanisme penegakan hukum yang kuat. Dengan demikian, studi terhadap kebijakan Amerika Serikat dapat menjadi acuan penting bagi Indonesia dalam memperbaiki kelemahan regulasi yang ada serta memastikan bahwa kebijakan yang disusun benar-benar mampu menjawab permasalahan yang ada secara konkret.

Pengaturan *cyber law* di Indonesia didasarkan pada beberapa peraturan perundang-undangan yang mengatur aktivitas di dunia maya. Regulasi utama yang menjadi landasan hukum adalah UU No. 19 Tahun 2016, yang merupakan perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).[16] Undang-undang ini mencakup aspek transaksi elektronik, data elektronik, serta tindak pidana siber. Beberapa tindak pidana siber yang diatur meliputi penyebaran konten ilegal seperti pornografi, perjudian online, dan pencemaran nama baik, serta tindakan akses ilegal ke sistem elektronik, intersepsi atau penyadapan tanpa izin, dan perusakan sistem elektronik.[17] Selain itu, pengaturan mengenai transaksi elektronik dalam *cyber law* Indonesia mencakup keabsahan kontrak elektronik, tanda tangan elektronik, serta sertifikat elektronik. Perlindungan data pribadi juga menjadi perhatian utama dengan adanya kewajiban bagi penyelenggara sistem elektronik untuk menjaga keamanan data pengguna.

Selain UU ITE, dalam UU No. 1 Tahun 2023 tentang KUHP, yang akan berlaku pada tahun 2026, terdapat beberapa ketentuan terkait *cyber law*. Beberapa regulasi lain yang turut

[16] Adinda Lola Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia," *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (July 18, 2024): 69–77, https://doi.org/10.58707/aldalil.v2i2.777.

[17] H. Abdul Wahid, *Kejahatan Mayantara (Cyber Crime)*, (Bandung: Refika Aditama, 2005), 146.

berperan dalam pengaturan *cyber law* di Indonesia adalah UU No. 44 Tahun 2008 tentang Pornografi, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta berbagai peraturan dari Kementerian Komunikasi dan Informatika (Kominfo) terkait penyelenggaraan sistem elektronik.

Meskipun telah memiliki berbagai regulasi, pengaturan *cyber law* di Indonesia masih menghadapi beberapa tantangan. Perkembangan teknologi yang sangat cepat membuat hukum harus terus beradaptasi dengan perubahan digital. Selain itu, isu yurisdiksi lintas batas negara menjadi tantangan dalam penegakan hukum terhadap pelaku kejahatan siber yang berada di luar negeri. Terakhir, diperlukan keseimbangan antara kebebasan berekspresi dan perlindungan kepentingan umum agar regulasi tidak disalahgunakan untuk membatasi hak-hak digital masyarakat.[18]

Berikutnya mengenai optimalisasi pengaturan dan pencegahan *cyber crime* di Indonesia dilakukan melalui berbagai upaya dalam aspek hukum, penegakan hukum, teknis, serta edukasi masyarakat. Kerangka hukum *cyber crime* di Indonesia berlandaskan pada UU Informasi dan Transaksi Elektronik (UU ITE)[19], khususnya Pasal 27-37 yang mengatur berbagai bentuk kejahatan siber, seperti konten ilegal, akses ilegal, dan manipulasi data. Selain itu, Pasal 45 UU No. 1 Tahun 2023 menetapkan sanksi pidana hingga 10 tahun penjara dan denda maksimal Rp10 miliar untuk tindak pidana perjudian online. Pengaturan mengenai *cyberbullying* juga menjadi perhatian, di mana Pasal 27 ayat (3) dan (4) UU ITE serta Pasal 27A dan 27B dalam perubahan UU ITE secara khusus mengatur penghinaan, pencemaran nama baik, pemerasan, dan pengancaman melalui sistem elektronik.[20] Sanksi pidana terhadap pelaku *cyberbullying* diatur dalam Pasal 45 ayat (4) dengan ancaman maksimal 2 tahun penjara dan/atau denda hingga Rp400 juta.

Dalam upaya optimalisasi pengaturan *cyber crime*, diperlukan penguatan regulasi, termasuk harmonisasi peraturan perundang-undangan terkait kejahatan siber, penyesuaian dengan perkembangan teknologi informasi, serta pengaturan yurisdiksi yang lebih jelas untuk mengatasi sifat lintas batas kejahatan ini.[21] Di sisi penegakan hukum, peningkatan kapasitas penyidik khusus *cyber crime* sesuai dengan Pasal 43 UU ITE menjadi hal yang penting, termasuk optimalisasi kewenangan penyidik dalam memerintahkan

[18] Galih Eko Kurniawan, "Opini: Urgensi UU Keamanan Dan Ketahanan Siber," *Harianjogja.Com*, October 8, 2019, accessed March 15, 2025, https://opini.harianjogja.com/read/2019/10/08/543/1021151/opini-urgensi-uu-keamanan-dan-ketahanansiber

[19] Sulasi Rongiyati. (2021). Urgensi Sinergitas Pengaturan Perlindungan Data Pribadi dan Keamanan Siber Nasional. Info Singkat: Kajian Singkat Terhadap Isu Aktual dan Strategis, 13(11), 1-6.

[20] Adami Chazawi, Hukum Pidana Positif Penghinaan, Edisi Revisi (Malang: Media Nusa Creative, 2013), 81.

[21] Sigid Suseno, Yurisdiksi Tindak Pidana Siber (Bandung: Refika Aditama, 2012), 177–178.

pemutusan akses sementara terhadap akun media sosial, rekening bank, dan aset digital. Selain itu, implementasi kerja sama internasional dalam penyidikan sesuai dengan Pasal 43 ayat (8) UU ITE juga diperlukan untuk menghadapi tantangan global dalam kejahatan siber.

Pencegahan *cyber crime* dilakukan melalui beberapa pendekatan. Dari segi teknis, penguatan sistem keamanan siber nasional, pengembangan teknologi deteksi dini, serta implementasi sistem pemantauan konten ilegal menjadi langkah penting.[22] Dari segi hukum dan kelembagaan, pembentukan tim khusus di setiap wilayah serta penerapan Pasal 36 Permenkominfo No. 5/2020 terkait akses data elektronik untuk kepentingan penegakan hukum dapat meningkatkan efektivitas pencegahan. Peningkatan koordinasi antar lembaga penegak hukum juga menjadi kunci keberhasilan penanganan *cyber crime*. Pendekatan sosial dan edukasi pun tidak kalah penting, dengan adanya sosialisasi mengenai dampak kejahatan siber, edukasi literasi digital, serta pemberdayaan masyarakat untuk aktif melaporkan kasus *cyber crime*.

Meskipun telah dilakukan berbagai upaya, masih terdapat tantangan dalam pencegahan dan penanganan *cyber crime*, seperti perkembangan teknologi yang pesat, sifat lintas batas kejahatan siber, serta kesulitan dalam pembuktian dan identifikasi pelaku.[23] Untuk mengatasi tantangan tersebut, diperlukan evaluasi dan pembaruan regulasi secara berkala, penguatan kerja sama internasional dalam penegakan hukum siber, serta investasi pada teknologi dan sumber daya manusia yang berkualitas dalam menangani *cyber crime*. Dengan langkah-langkah ini, diharapkan pengaturan dan pencegahan kejahatan siber di Indonesia semakin optimal dan mampu memberikan perlindungan yang lebih baik bagi masyarakat di era digital.

Amerika Serikat menerapkan pendekatan komprehensif dalam pengaturan dan pencegahan *cyber crime* dengan mengandalkan kerangka hukum federal yang kuat, optimalisasi penegakan hukum, strategi pencegahan, serta inovasi teknologi. Pada tingkat kerangka hukum federal, beberapa undang-undang utama menjadi dasar dalam menangani kejahatan siber. *Computer Fraud and Abuse Act (CFAA)* merupakan regulasi utama yang mengatur akses tidak sah ke sistem komputer dengan sanksi pidana hingga 20 tahun penjara untuk pelanggaran serius.[24] *Electronic Communications Privacy Act (ECPA)* melindungi komunikasi elektronik dari penyadapan dan akses ilegal, sekaligus mengatur prosedur resmi bagi penegak hukum dalam melakukan pengawasan

[22] Yudho Winarto, "RUU Keamanan Dan Ketahanan Siber," *nasional.kontan.co.id*, 2022, accessed March 15, 2025, https://nasional.kontan.co.id/news/kominfo-dukung-ruukeamanan-ketahanan-siber-untuk-lengkapi-uu-ite

[23] Dista Amalia Arifah, "Kasus *Cybercrime* di Indonesia," Jurnal Bisnis dan Ekonomi (JBE) 18, no. 2 (September 2011): 189.

[24] Leahy, G. F. (2022). Keeping Gates Down: Further Narrowing the Computer Fraud and Abuse Act in the Wake of Van Buren.Wm. & Mary Bus. L. Rev.,14, 215.

elektronik. Selain itu, *Identity Theft Enforcement* and *Restitution Act* memperluas yurisdiksi federal untuk kasus pencurian identitas dan memungkinkan korban mendapatkan restitusi atas waktu yang mereka habiskan dalam memulihkan identitas mereka.

Dalam optimalisasi penegakan hukum, berbagai lembaga berperan aktif dalam menangani *cyber crime*. *FBI Cyber Division* menjadi ujung tombak dalam penegakan hukum di tingkat federal, sementara Secret *Service Electronic Crimes Task Forces* berfokus pada kejahatan finansial digital. Koordinasi antar lembaga dilakukan melalui *National Cyber Investigative Joint Task Force (NCIJTF)* untuk menangani ancaman siber secara efektif. Mengingat kejahatan siber seringkali melibatkan banyak yurisdiksi, *Internet Crime Complaint Center (IC3)* berfungsi sebagai pusat pelaporan nasional, dengan koordinasi antara lembaga penegak hukum federal, negara bagian, dan lokal. Untuk kasus lintas negara, Amerika Serikat menggunakan *Mutual Legal Assistance Treaties (MLAT)* guna mempercepat kerja sama investigasi dengan negara lain.[25] Bantuan Hukum Timbal Balik (*Mutual Legal Assistance*), pada dasarnya adalah suatu mekanisme formal dimana suatu negara dapat meminta negara lain/lembaga luar negeri untuk memberikan bantuan guna penyidikan, penuntutan, pengadilan suatu perkara pidana. [26] Undang-undang 1/2006 tentang Bantuan Timbal Balik mengatur secara rinci mengenai permintaan bantuan timbal balik dalam masalah pidana dari Pemerintah Republik Indonesia kepada negara diminta antara lain menyangkut pengajuan permintaan bantuan, persyaratan permintaan, bantuan untuk mencari atau mengidentifikasi orang, bantuan untuk mendapatkan alat bukti, dari bantuan untuk mengupayakan kehadiran orang.

Strategi pencegahan *cyber crime* dilakukan melalui kemitraan publik-swasta, edukasi, dan inovasi teknologi. *Information Sharing and Analysis Centers (ISACs)* berperan dalam berbagi informasi ancaman siber, sementara *Cybersecurity and Infrastructure Security Agency (CISA)* menyediakan panduan bagi perusahaan dan individu untuk meningkatkan keamanan siber.[27] Selain itu, *National Cyber Security Alliance* berfokus pada edukasi masyarakat dan bisnis mengenai ancaman siber. Dari sisi edukasi, program seperti *"Stop.Think.Connect"* bertujuan meningkatkan kesadaran keamanan siber, sementara pelatihan keamanan siber bagi penegak hukum dan

[25] Stigall, Dan. "Countering Convergence: "Central Authorities" and the Global Network to Combat Transnational Crime and Terrorism"

[26] Rona, Nabella (2024) "Perjanjian Ekstradisi Dalam Penegakan Hukum
Tindak Pidana Korupsi Di Indonesia" https://yustitia.unwir.ac.id/index.php/yustitia/article/download/123/107/281

[27] Mark MacCarthy, Ian Seyal Eduardo Levy Yeyati, and Tom Wheeler, "The Military Role in National Cybersecurity Governance," *Brookings*, accessed March 15, 2025, http://www.brookings.edu/research/opinions/2013/12/16military-role-national-cybersecurity-governance-wallace. Diakses September 2014.

profesional IT semakin diperluas.[28] Institusi pendidikan juga memasukkan kurikulum keamanan siber untuk membekali generasi mendatang dalam menghadapi ancaman digital. Dalam aspek inovasi, pemerintah federal berinvestasi dalam pengembangan teknologi deteksi dini dan alat forensik digital guna meningkatkan efektivitas investigasi serta implementasi sistem peringatan dini terhadap serangan siber.[29]

Meskipun sistem pengaturan dan pencegahan *cyber crime* di Amerika Serikat sudah cukup maju, masih terdapat beberapa tantangan yang harus diatasi. Dari segi yurisdiksi, kerja sama internasional terus dikembangkan melalui Konvensi Budapest tentang *Cybercrime*, serta peningkatan kapasitas diplomatik dalam menangani kejahatan siber lintas negara. Dari perspektif perlindungan privasi, diperlukan keseimbangan antara penegakan hukum dan hak privasi warga negara, dengan pengawasan ketat oleh pengadilan terhadap penggunaan alat investigasi digital.[30] Sementara itu, dalam menghadapi perkembangan teknologi baru, regulasi terus diperbarui untuk mengakomodasi inovasi seperti *cryptocurrency* dan *Internet of Things (IoT)*, serta memastikan pelatihan berkelanjutan bagi penegak hukum agar tetap relevan dalam menangani ancaman siber yang terus berkembang.

Perbandingan optimalisasi pengaturan *cyber law* dan pencegahan *cyber crime* di Indonesia dan Amerika Serikat menunjukkan perbedaan signifikan dalam pendekatan regulasi, kelembagaan, serta strategi pencegahan dan penegakan hukum. Dari segi kerangka hukum, Indonesia menggunakan pendekatan terpusat dengan UU ITE sebagai regulasi utama yang mencakup berbagai aspek kejahatan siber, sementara Amerika Serikat mengadopsi pendekatan sektoral, di mana berbagai undang-undang federal seperti CFAA, ECPA, dan DMCA digunakan untuk menangani kasus *cyber crime* sesuai dengan sektor yang terlibat. Selain itu, AS juga memiliki regulasi khusus di tingkat negara bagian serta aturan sektoral seperti HIPAA untuk kesehatan dan GLBA untuk keuangan, yang belum diterapkan di Indonesia.

Dari sisi struktur kelembagaan, Indonesia masih dalam tahap pengembangan dengan rencana pembentukan badan siber melalui RUU KKS 2025, sementara AS telah memiliki struktur komprehensif dengan lembaga seperti *FBI Cyber Division*,

[28] National Cyber Security Alliance, Stop.Think.Connect, [Online]. Available: www.stopthinkconnect.org/

[29] Kementerian Komunikasi Dan Digital, "Siaran Pers No. 83/PIH/KOMINFO/11/2013 Tentang Ancaman Cyber Attack Dan Urgensi Keamanan Informasi Nasional," *Komdigi.Go.Id*, accessed March 15, 2025, https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-83-pih-kominfo-11-2013-tentang-ancaman-cyber-attack-dan-urgensi-keamanan-informasi-nasional.

[30] Moch. Marsa Taufiqurrohman, "Meninjau Urgensi Undang-Undang Keamanan Dan Ketahanan Siber Di Indonesia," *KOMPASIANA*, accessed March 15, 2025, https://www.kompasiana.com/mochmarsa_t/5ea77147d541df16d93dab72/meninjau-urgensi-undang-undang-keamanan-dan-ketahanan-siber-diindonesia?page=2&page_images=1

Secret Service Electronic Crimes Task Forces, dan *NCIJTF*, yang berkoordinasi secara efektif dalam menangani kejahatan siber.[31] AS juga memiliki *Internet Crime Complaint Center (IC3)* sebagai pusat pelaporan nasional yang terintegrasi, sedangkan Indonesia masih memiliki koordinasi yang terbatas antar lembaga penegak hukum.

Dalam aspek kewajiban pelaporan dan perlindungan infrastruktur, Indonesia melalui RUU KKS 2025 mulai menerapkan standar baru dengan kewajiban pelaporan insiden siber dalam waktu 3x24 jam dan penerapan kerangka keamanan siber bagi penyelenggara infrastruktur informasi.[32] Di sisi lain, AS telah lebih maju dengan sistem *Information Sharing and Analysis Centers (ISACs)* yang memungkinkan sektor swasta berbagi informasi ancaman siber, serta *Cybersecurity and Infrastructure Security Agency (CISA)* yang menyediakan standar keamanan siber di tingkat federal. Kemitraan publik-swasta dalam pertukaran informasi ancaman siber juga menjadi keunggulan AS dalam menghadapi ancaman siber yang terus berkembang.

Dalam pendekatan pencegahan, Indonesia lebih berfokus pada penguatan sistem keamanan siber dan pembentukan tim khusus penanganan *cyber crime*, meskipun edukasi literasi digital masih terbatas. Sebaliknya, AS memiliki strategi pencegahan yang lebih sistematis dengan program edukasi nasional seperti *"Stop.Think.Connect"*[33], integrasi keamanan siber dalam kurikulum pendidikan, serta investasi besar dalam teknologi deteksi dan pencegahan *cyber crime*.

Tantangan yang dihadapi kedua negara juga berbeda. Indonesia menghadapi perkembangan teknologi yang cepat, sifat lintas batas *cyber crime*, serta kesulitan dalam pembuktian kasus, yang coba diatasi dengan penguatan regulasi melalui RUU KKS (Keamanan dan Ketahanan Siber) 2025. Sementara itu, AS menghadapi tantangan yurisdiksi lintas negara, yang diatasi melalui Konvensi Budapest tentang *Cybercrime*,[34] serta dilema keseimbangan antara privasi dan penegakan hukum, yang dijawab dengan pengawasan pengadilan terhadap investigasi digital dan pembaruan regulasi untuk mengakomodasi teknologi baru.[35]

Secara keseluruhan, Indonesia sedang bergerak ke arah penguatan kerangka hukum melalui RUU KKS 2025, tetapi masih perlu meningkatkan

[31] P. Schwartz, "Scenarios for the future of cyber security," America's Cyber Future, vol. 2, pp. 217–228, 2011.

[32] Hukumonline, "Ruu KKS 2025: Kewajiban Pelaporan Insiden Siber Baru Bagi Penyelenggara," *Hukumonline.Com*, Februari 21, 2025, accessed March 15, 2025, https://pro.hukumonline.com/a/lt67b7e7443afc2/ruu-kks-2025--kewajiban-pelaporan-insiden-siber-baru-bagi-penyelenggara

[33] T. Benzel, "A strategic plan for cybersecurity research and development," IEEE Security & Privacy, vol. 4, pp. 3–5, 2015.

[34] Spiezia, Filippo (05/2022). "International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime". *ERA Forum* (1612-3093), 23 (1), p. 101.

[35] D. Hodges and S. Creese, "Understanding cyber-attacks," Cyber warfare: A multidisciplinary analysis, pp. 33–60, 2015.

koordinasi antar lembaga serta kemitraan publik-swasta. Sementara itu, AS telah memiliki sistem yang lebih matang dengan pendekatan multi-sektor dan koordinasi yang kuat. Indonesia dapat mengambil pembelajaran dari model AS, terutama dalam membangun kemitraan publik-swasta, memperkuat sistem edukasi literasi digital, serta menerapkan standar keamanan siber yang lebih ketat untuk optimalisasi pengaturan dan pencegahan *cyber crime* di masa depan.

RUU KKS juga memiliki jaminan keamanan tersebut terutama diberikan terhadap potensi-potensi serangan siber *(cyber attacks)* seperti segala bentuk tindakan kejahatan di ranah siber, penyebaran *malware*, pencurian data pribadi, peretasan *(hacking)*, tindakan spionase siber dan lain sebagainya.[36]

B. Analisis Komparatif Kasus Peretasan Bjorka dalam Perspektif *Cyber Law* di Indonesia dan Amerika Serikat

Kasus peretasan Bjorka dapat dianalisis dalam perspektif *cyber law* Indonesia dengan mempertimbangkan penentuan *locus delicti* dan *tempus delicti*. Di Indonesia, *locus delicti* dapat ditentukan berdasarkan beberapa teori yang juga diterapkan di Amerika Serikat, yaitu teori *uploader* dan *downloader* yang menekankan lokasi pelaku dan korban, teori *law of the server* yang memperlakukan server sebagai tempat kejadian, serta teori *international space* yang menganggap dunia maya sebagai lingkungan hukum tersendiri. Sementara itu, *tempus delicti* dapat ditentukan dengan mengacu pada *log file* yang mencatat berbagai aktivitas dalam sistem komputer. Dalam proses penyidikan, *Unit Cyber Crim*e Polri, sebagaimana disampaikan oleh Kombespol Dr. Petrus Golose, telah memiliki Standar Operasional Prosedur (SOP) yang mengacu pada standar internasional, termasuk prosedur yang digunakan oleh FBI di Amerika Serikat. Proses penyidikan melibatkan tahapan *acquiring* dan *imaging*, yakni penggandaan barang bukti digital secara presisi, serta analisis data, termasuk data yang telah dihapus, disembunyikan, dienkripsi, dan jejak *log file*. Dasar hukum utama yang digunakan dalam menangani kasus seperti Bjorka adalah UU ITE (UU No. 11 Tahun 2008 *jo.* UU No. 19 Tahun 2016), terutama Pasal 30-33 yang mengatur akses ilegal dan manipulasi data, serta Pasal 43 UU ITE yang memberikan kewenangan penyidikan kepada aparat penegak hukum. Didalam dapat dikenakan Pasal 88 RUU PKS Bjorka dapat dikenakan tindak pidana 15 tahun dan denda Rp 15 Miliar.[37]

[36] Naskah Akademik RUU Keamanan dan Ketahanan Siber (RUU PKS) (2019) (https://berkas.dpr.go.id/akd/dokumen/RJ1-20190617-025848-5506.pdf

[37] Pasal 88 RUU Keamanan dan Ketahanan Siber berbunyi, "Setiap Orang yang dengan sengaja dan melawan hukum melakukan serangan dan/atau peretasan Siber dengan maksud membuat kerusakan, gangguan, atau penghentian layanan IIK, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan/atau denda paling banyak Rp15.000.000.000,00 (lima belas miliar rupiah)." https://www.hukumonline.com/pusatdata/detail/lt67b424f918b8c/rancangan-undang-undang-tahun-2025/

Dalam perbandingan dengan Amerika Serikat, pendekatan hukum yang digunakan oleh Indonesia lebih terpusat dengan UU ITE sebagai payung hukum utama, sementara Amerika Serikat mengadopsi pendekatan sektoral dengan berbagai undang-undang, seperti *Computer Fraud and Abuse Act (CFAA)* yang secara khusus mengatur akses tidak sah ke sistem komputer.[38] Dalam hal akses data untuk penegakan hukum, Indonesia mewajibkan PSE Lingkup Privat untuk memberikan akses kepada aparat hukum berdasarkan Pasal 36 Permenkominfo No. 5/2020 , dengan prosedur yang mensyaratkan dasar kewenangan, maksud dan tujuan, serta deskripsi data yang diperlukan. Di Amerika Serikat, akses terhadap data diatur lebih rinci melalui *Electronic Communications Privacy Act (ECPA*), yang mewajibkan adanya surat perintah pengadilan (*warrant*) untuk mengakses konten komunikasi, serta mekanisme *National Security Letter* untuk kasus yang berkaitan dengan keamanan nasional.[39] Dari segi koordinasi antar lembaga, Indonesia masih dalam tahap pengembangan dengan melibatkan ahli digital forensik dari Polri dan pakar eksternal, sementara Amerika Serikat telah memiliki struktur koordinasi yang lebih matang melalui *National Cyber Investigative Joint Task Force (NCIJTF)*, yang mengkoordinasikan berbagai lembaga federal dalam penanganan kasus siber.[40]

Penanganan kasus Bjorka juga menghadapi berbagai tantangan, terutama dalam aspek yurisdiksi dan pembuktian. Kejahatan siber yang bersifat lintas batas sering kali menyulitkan penentuan yurisdiksi, terutama jika pelaku berada di luar negeri, sehingga Indonesia perlu memperkuat kerja sama internasional dalam penegakan hukum siber. Selain itu, pembuktian digital juga menjadi tantangan karena bukti dapat dengan mudah diubah, disadap, dipalsukan, atau disebarkan ke berbagai lokasi dalam waktu singkat. Oleh karena itu, diperlukan penguatan kapasitas forensik digital guna menganalisis bukti elektronik secara akurat. Kesimpulannya, kasus Bjorka menunjukkan urgensi untuk memperkuat kerangka hukum siber di Indonesia, khususnya dalam aspek penyidikan dan pembuktian digital. Amerika Serikat, dengan pengalaman yang lebih panjang dalam menangani kejahatan siber, memiliki sistem yang lebih matang dengan pendekatan multi-sektor dan koordinasi yang kuat antar lembaga. Indonesia dapat mengadopsi praktik terbaik dari Amerika Serikat dalam pengembangan regulasi *cyber law* serta peningkatan efektivitas penegakan hukum dalam menangani kejahatan siber.

[38] Soullier, B. A. (2023). Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren.Fed. Comm. LJ,76, 239.

[39] Electronic Communications Privacy Act. (1986). Pub. L. No. 99-508, 100 Stat. 1848. Retrieved from https://www.congress.gov/bill/99th-congress/house-bill/4952.

[40] National cyber investigative joint task force releases ransomware fact sheet. (2021). *Computer and Internet Lawyer*, *38*(5), 22. Retrieved from https://www.proquest.com/trade-journals/national-cyber-investigative-joint-task-force/docview/2630359675/se-2

Kasus peretasan dan pembocoran data yang dilakukan oleh Bjorka dapat dianalisis berdasarkan berbagai ketentuan dalam *cyber law* Amerika Serikat. Salah satu undang-undang utama yang dapat digunakan adalah *Computer Fraud and Abuse Act (CFAA)*, yang mengatur tentang akses tidak sah ke sistem komputer.[41] Berdasarkan 18 U.S.C. § 1030(a)(2), Bjorka dapat dijerat karena dengan sengaja mengakses komputer tanpa otorisasi untuk memperoleh informasi, khususnya data pribadi dan dokumen rahasia dari sistem pemerintah yang dikategorikan sebagai *"protected computer"*.[42] Selain itu, berdasarkan 18 U.S.C. § 1030(a)(5), tindakan peretasan yang menyebabkan gangguan pada sistem dan kerugian ekonomi juga dapat dikenai sanksi, mengingat prinsip utama dalam undang-undang ini adalah perlindungan otorisasi dan integritas sistem komputer.

Selain *CFAA, Electronic Communications Privacy Act (ECPA)* juga relevan dalam kasus ini, terutama dalam aspek penyadapan dan akses tidak sah ke komunikasi elektronik. Berdasarkan 18 U.S.C. § 2511[43], Bjorka dapat dijerat karena dengan sengaja menyadap, menggunakan, atau mengungkapkan komunikasi elektronik tanpa otorisasi, yang melanggar prinsip kerahasiaan komunikasi dan perlindungan privasi individu. Lebih lanjut, 18 U.S.C. § 2701[44] mengatur akses tidak sah terhadap komunikasi tersimpan, seperti email atau data yang disimpan di server layanan komunikasi. Dengan adanya tindakan memperoleh dan menyebarluaskan informasi tanpa izin, aspek kepemilikan informasi dan keamanan penyimpanan data juga menjadi poin utama dalam pelanggaran ini.

Dalam perspektif keamanan ekonomi dan perlindungan data strategis, *Economic Espionage Act* melalui 18 U.S.C. § 1831[45] juga dapat diterapkan jika peretasan yang dilakukan oleh Bjorka terbukti menguntungkan pihak asing atau melibatkan informasi yang bernilai ekonomi tinggi. Aspek ekonomi dan keamanan nasional menjadi perhatian utama, mengingat prinsip perlindungan aset intelektual dan kedaulatan informasi negara harus dijaga dari ancaman eksternal. Selain itu, karena kasus ini juga melibatkan pencurian data pribadi, *Identity Theft and Assumption Deterrence Act* melalui 18 U.S.C. § 1028[46] dapat digunakan untuk menjerat tindakan memperoleh,

[41] Kane, S. (2020). Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act. *The University of Chicago Law Review, 87*(5), 1437-1477. https://www.proquest.com/scholarly-journals/available-granted-revoked-new-framework-assessing/docview/2425612708/se-2

[42] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers https://www.law.cornell.edu/uscode/text/18/1030

[43] 18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited https://www.law.cornell.edu/uscode/text/18/2511

[44] 18 U.S. Code § 2701 - Unlawful access to stored communications https://www.law.cornell.edu/uscode/text/18/2701

[45] 18 U.S. Code § 1831 - Economic espionage https://www.law.cornell.edu/uscode/text/18/1831

[46] 18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information https://www.law.cornell.edu/uscode/text/18/1028

memiliki, atau menyebarluaskan informasi identitas orang lain tanpa izin.[47] Dalam hal ini, pencurian data NIK, KK, dan informasi pribadi lainnya dianggap sebagai pelanggaran serius terhadap prinsip perlindungan identitas dan tanggung jawab data. Dalam konteks Amerika Serikat, kasus Bjorka ditangani oleh *Cyber Division* dengan koordinasi melalui *National Cyber Investigative Joint Task Force (NCIJTF)*. Struktur koordinasi yang lebih matang ini memungkinkan pendekatan multi-lembaga yang lebih efektif dibandingkan dengan sistem yang diterapkan di Indonesia. Dengan berbagai undang-undang yang lebih spesifik dan prosedur penegakan hukum yang lebih terstruktur, Amerika Serikat memiliki sistem yang lebih komprehensif dalam menangani kasus *cyber crime* seperti peretasan dan pembocoran data yang dilakukan oleh Bjorka.

Dengan demikian, untuk memperkuat keamanan siber dan mencegah terjadinya kebocoran data, langkah-langkah yang bisa diambil oleh pemerintah Indonesia adalah pertama, pembentukan lembaga yang berperan sebagai pengawas terhadap pengendali data pribadi. Kedua, pengesahan RUU KKS yang berfungsi dalam penguatan hal-hal teknis berkaitan dengan keamanan siber. Dan ketiga, kerjasama penguatan kerjasama antar lembaga seperti NCIJTF yang berperan dalam kejahatan siber.

D. PENUTUP

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa regulasi *cybercrime* di Indonesia, khususnya dalam kasus Bjorka, masih memiliki beberapa kelemahan dalam aspek yurisdiksi, mekanisme penegakan hukum, dan perlindungan infrastruktur informasi kritis. UU ITE dan UU PDP belum sepenuhnya mengakomodasi perkembangan teknologi serta modus operandi kejahatan siber yang semakin kompleks dan lintas batas negara. Dibandingkan dengan Amerika Serikat, Indonesia masih tertinggal dalam hal kerangka hukum dan kerja sama internasional dalam menangani kejahatan siber. Oleh karena itu, perlu adanya reformasi regulasi yang lebih komprehensif untuk mengoptimalkan penegakan hukum di era digital.
Sehingga, Tim Peneliti mengambil beberapa saran yaitu;

Pertama, pengesahan RUU KKS yang berperan dalam meningkatkan standar keamanan siber. Walaupun terdapat aspek yang perlu ditingkatkan seperti kurangnya koordinasi dengan antar lembaga-lembaga seperti contohnya NCIJTF yang berperan dalam kejahatan siber. Namun, RUU KKS bisa mengurangi potensi-potensi serangan siber seperti *hacking*.

Kedua, Indonesia juga perlu memperkuat kerja sama dengan negara lain dalam hal seperti ekstradisi untuk mempermudah menangkap dan mengadili pelaku kejahatan siber.

[47] Guffey, C. A. (2019). *Customer Authentication in the Payment Industry* (Order No. 13865720). Available from ProQuest Dissertations & Theses Global. (2219369436). https://www.proquest.com/dissertations-theses/customer-authentication-payment-industry/docview/2219369436/se-2

Selain itu, diperlukan penerapan MLA (*Mutual Legal Assistance*) untuk mempermudah investigasi agar penindakan dan pencegahan dapat dilakukan dengan efektif.

Ketiga, peningkatan sosialisasi kesadaran data pribadi dan peningkatan literasi masyarakat. Masyarakat harus diberikan edukasi terkait ancaman kejahatan siber, khususnya dalam hal keamanan data pribadi dan pencegahan serangan siber. Kampanye literasi digital yang melibatkan berbagai pemangku kepentingan perlu ditingkatkan untuk mengurangi risiko kejahatan siber di Indonesia

DAFTAR PUSTAKA

18 U.S. Code § 1030 - Fraud and related activity in connection with computers https://www.law.cornell.edu/uscode/text/18/1030

18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited https://www.law.cornell.edu/uscode/text/18/2511

18 U.S. Code § 2701 - Unlawful access to stored communications https://www.law.cornell.edu/uscode/text/18/2701

18 U.S. Code § 1831 - Economic espionage https://www.law.cornell.edu/uscode/text/18/1831

18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information https://www.law.cornell.edu/uscode/text/18/1028

Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara (*Cyber Crime*) (Bandung: Refika Aditama, 2005), 146.

Adami Chazawi, Hukum Pidana Positif Penghinaan, Edisi Revisi (Malang: Media Nusa Creative, 2013), 81.

Antonius Galih Prasetyo, "Prasyarat Keberhasilan Dan Nilai Tambah 'Super App,'" Kompas.Id, July 31, 2022, accessed March 15, 2025, https://www.kompas.id/baca/opini/2022/07/28/prasyarat-keberhasilan-dan-nilai-tambah-super-app

Arifah, D. A. (2011). Kasus cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi (JBE)*, *18*(2).

Benzel, T. (2015). A strategic plan for cybersecurity research and development. *IEEE Security & Privacy*, *4*, 3–5.

Chazawi, A. (2013). *Hukum pidana positif penghinaan* (Edisi Revisi). Malang: Media Nusa Creative.

Databoks.katadata.co.id. (2022). Indonesia masuk 3 besar negara dengan kasus kebocoran data terbanyak dunia: Databoks. Retrieved from https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/3f6a7dc0c5d0b7e/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia.

Desy Setyowati, "Daftar Data Diambil

Hacker Bjorka Dan Bahayanya Bagi Warga Indonesia," Teknologi Katadata.Co.Id, accessed March 15, 2025,https://katadata.co.id/digital/teknologi/631ec2eb7a23a/daftar-data-diambil-hacker-bjorka-dan-bahayanya-bagi-warga-indonesia

D. Hodges and S. Creese, "Understanding cyber-attacks," Cyber warfare: A multidisciplinary analysis, pp. 33–60, 2015.

Dinda, A. L. S. (2024). Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum*.

Dss. (n.d.). Sistem pemerintahan berbasis elektronik (SPBE). Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. Retrieved from https://www.menpan.go.id/site/kelembagaan/sistem-pemerintahan-berbasis-elektronik-spbe-2.

Electronic Communications Privacy Act. (1986). Pub. L. No. 99-508, 100 Stat. 1848. Retrieved from https://www.congress.gov/bill/99th-congress/house-bill/4952.

Farmita, Artika Rachmi, and Inge Klara Safitri. "Sosok Bjorka, Peretas Yang Mengacak-ACAK Sistem Data Indonesia." *Tempo.Co*. Tempo, September 12, 2022. Last modified September 12, 2022. Accessed March 15, 2025. https://www.tempo.co/infografik/infografik/sosok-bjorka-peretas-yang-mengacak-acak-sistem-data-indonesia-875.

Guffey, C. A. (2019). *Customer Authentication in the Payment Industry* (Order No. 13865720). Available from ProQuest Dissertations & Theses Global. (2219369436). https://www.proquest.com/dissertations-theses/customer-authentication-payment-industry/docview/2219369436/se-2

Hardiansyah, Z. (2022, September 7). Apa itu Breached Forums yang terlibat 4 kasus kebocoran data di Indonesia sebulan terakhir? Retrieved from https://tekno.kompas.com/read/2022/09/07/16150067/apa-itu-breached-forums-yang-terlibat-4-kasus-kebocoran-data-di-indonesia.

Hardiansyah, Z. (2022b, September 12). Rentetan aksi hacker Bjorka dalam kasus kebocoran data di Indonesia sebulan terakhir. *Kompas.com*. Retrieved from https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all.

Hodges, D., & Creese, S. (2015). Understanding cyber-attacks. In *Cyber warfare: A multidisciplinary analysis*.

Hukumonline (2025) RUU KKS 2025: Kewajiban Pelaporan Insiden Siber Baru Bagi Penyelenggara https://pro.hukumonline.com/a/lt67b7e7443afc2/ruu-kks-2025--kewajiban-pelaporan-insiden-siber-baru-bagi-penyelenggara

Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

https://peraturan.bpk.go.id/Details/101646/uud-no–.

Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara RI Tahun 2023 Nomor 1, Tambahan Lembaran RI Nomor 6842. Sekretariat Negara. Jakarta.

https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023.

Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008 Nomor 58, Tambahan Lembaran RI Nomor 4843. Sekretariat Negara. Jakarta.

https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-2008.

Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang perubahan UU ITE. Lembaran Negara RI Tahun 2016 Nomor 251, Tambahan Lembaran RI Nomor 5952. Sekretariat Negara. Jakarta.

https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016.

Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara RI Tahun 2022 Nomor 196, Tambahan Lembaran RI Nomor 6820. Sekretariat Negara. Jakarta.

https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

Kasia, J. (2025, January 6). Indeks SPBE nasional meningkat, Menteri Rini: Penguatan integrasi pelayanan publik berbasis digital. Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. Retrieved from https://www.menpan.go.id/site/berita-terkini/indeks-spbe-nasional-meningkat-menteri-rini-penguatan-integrasi-pelayanan-publik-berbasis-digital.

Kane, S. (2020). Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act. *The University of Chicago Law Review*, *87*(5), 1437-1477. https://www.proquest.com/scholarly-journals/available-granted-revoked-new-framework-assessing/docview/2425612708/se-2

Kementerian Komunikasi dan Informatika Republik Indonesia. (2013). Ancaman cyber attack dan urgensi keamanan informasi nasional. Retrieved from https://www.kominfo.go.id/index.php/content/detail/3479

Kurniawan, Galih Eko. (2019). OPINI: Urgensi UU Keamanan dan Ketahanan Siber. Available online from:https://opini.harianjogja.com/read/2019/10/08/543/1021151/opini-urgensi-uu-keamanan-dan-ketahanansiber

Leahy, G. F. (2022). Keeping gates down:Further narrowing the Computer Fraud and Abuse Act in the wake of Van Buren. *William & Mary Business Law Review, 14*.

National Cyber Security Alliance, Stop.Think.Connect,. [Online]. Available: www.stopthinkconnect.org/

Naskah Akademik RUU Keamanan dan Ketahanan Siber (RUU PKS) (2019) (https://berkas.dpr.go.id/akd/dokumen/RJ1-20190617-025848-5506.pdf

Marsa, M. (2022). Meninjau urgensi Undang-Undang Keamanan dan Ketahanan Siber di Indonesia. Retrieved from https://www.kompasiana.com/mochmarsa_t/5ea77147d541df16d93dab72/meninjau-urgensi-undang-undang-keamanan-dan-ketahanan-siber-di-indonesia?page=2&page_images=1.

Melynda Dwi Puspita and Grace gandhi, "Nama Bjorka Disebut-Sebut Dalam Pembobolan 6 Juta NPWP, Ada Data Milik Jokowi, Gibran, Hingga Sri Mulyani," Tempo, September 19, 2024, accessed March 15, 2025, https://www.tempo.co/ekonomi/nama-bjorka-disebut-sebut-dalam-pembobolan-6-juta-npwp-ada-data-milik-jokowi-gibran-hingga-sri-mulyani--8048

National cyber investigative joint task force releases ransomware fact sheet. (2021). *Computer and Internet Lawyer*, *38*(5), 22. Retrieved from https://www.proquest.com/trade-journals/national-cyber-investigative-joint-task-force/docview/2630359675/se-2

P. Schwartz, "Scenarios for the future of cyber security," America's Cyber Future, vol. 2, pp. 217–228, 2011.

PERPRES No. 18 Tahun 2020. (n.d.). *Database Peraturan | JDIH BPK*. Retrieved from https://peraturan.bpk.go.id/Details/131386/perpres-no-18-tahun-2020.

PERPRES No. 95 Tahun 2018. (n.d.). *Database Peraturan | JDIH BPK*. Retrieved from https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018.

Prasetyo, A. G. (2022). Prasyarat keberhasilan dan nilai tambah "Super App." Retrieved from https://www.kompas.id/baca/opini/2022/07/28/prasyarat-keberhasilan-dan-nilai-tambah-super-app.

Puspita, M. D., & Gandhi, G. (2024, September 19). Nama Bjorka disebut-sebut dalam pembobolan 6 juta NPWP. *Tempo*. Retrieved from https://www.tempo.co/ekonomi/nama-bjorka-disebut-sebut-dalam-pembobolan-6-juta-npwp-ada-data-milik-jokowi-gibran-hingga-sri-mulyani--804.

Rona, Nabella (2024) "Perjanjian Ekstradisi Dalam Penegakan Hukum Tindak Pidana Korupsi Di Indonesia" https://yustitia.unwir.ac.id/index.php/yustitia/article/download/123/107/281

Rongiyati, S. (2021). Urgensi sinergitas pengaturan perlindungan data pribadi dan keamanan siber nasional. *Info Singkat: Kajian Singkat Terhadap Isu Aktual dan Strategis*.

Schwartz, P. (2011). Scenarios for the future of cybersecurity. *America's Cyber Future*.

Sigid Suseno, Yurisdiksi Tindak Pidana Siber (Bandung: Refika Aditama, 2012), 177–78.

Soullier, B. A. (2023). Decriminalizing

trivial computer use: The need to narrow the Computer Fraud and Abuse Act (CFAA) after Van Buren. *Federal Communications Law Journal, 76*.

Suseno, S. (2012). *Yurisdiksi tindak pidana siber*. Bandung: Refika Aditama

Sulasi Rongiyati. (2021). Urgensi Sinergitas Pengaturan Perlindungan Data Pribadi dan Keamanan Siber Nasional. Info Singkat: Kajian Singkat Terhadap Isu Aktual dan Strategis, 13(11), 1-6.

Soullier, B. A. (2023). Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren.Fed. Comm. LJ,76, 239.

Spiezia, Filippo (05/2022). "International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime". *ERA Forum* (1612-3093), 23 (1), p. 101.

Stigall, D. (2016). Countering convergence: "Central authorities" and the global network to combat transnational crime and terrorism. Air and Space Power Journal - Afrique & Francophonie, 1st Quarter 2016. George Washington University - Law School; U.S. Department of Justice.

T. Benzel, "A strategic plan for cybersecurity research and development," IEEE Security & Privacy, vol. 4, pp. 3–5, 2015.

Thantawi. (2014). Perlindungan korban tindak pidana cyber crime dalam sistem hukum pidana Indonesia. *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala, 2*(1).

United States Code. (n.d.). Title 18 - Crimes and criminal procedure. Retrieved from https://www.law.cornell.edu/uscode/text/18.

Wahid, A., & Labib, M. (2005). *Kejahatan mayantara (cyber crime)*. Bandung: Refika Aditama.

Wahyuni, W. (n.d.). Jerat Hukum Peretasan oleh Hacker. Retrieved from https://www.hukumonline.com/berita/a/jerat-hukum-peretasan-oleh-hacker-lt631ec0ed9e52c

Wallace, I. (2013). The military role in national cybersecurity governance. *Brookings*.

Winarto, Yudho. (2022). RUU Keamanan dan Ketahanan Siber. Availabe online from: https://nasional.kontan.co.id/news/kominfo-dukung-ruukeamanan-ketahanan-siber-untuk-lengkapi-uu-ite.8Marsa

Zulfikar Hardiansyah, "APA ITU Breached Forums Yang Terlibat 4 Kasus Kebocoran Data Di Indonesia Sebulan Terakhir?," KOMPAS.Com, September 7, 2022, accessed March 15, 2025,https://tekno.kompas.com/read/2022/09/07/16150067/apa-itu-breached-forums-yang-terlibat-4-kasus-kebocoran-data-di-indonesia

Hacker Bjorka Dalam Kasus Kebocoran Data Di Indonesia Sebulan Terakhir Halaman All," KOMPAS.Com, September 12, 2022,

accessed March 15, 2025, https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all