CENDEKIA: Jurnal Hukum, Sosial & Humaniora
Volume 2, Issue 4, 2024
E-ISSN: 2985-9174
https://doi.org/10.5281/zenodo.13883603

Kejahatan Siber (*Cyber Crime*) dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI)

Muhammad Ghozali[1*], Nora Liana[2], Cut Afra[3], Zulfadly Siregar[4], Nurfahni[5] Malahayati[6] & Muhammad Hatta[7]

[1], [2], [3], [4], [5] *Mahasiswa Program Studi Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Aceh, Indonesia*

[6], [7] *Dosen Program Studi Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Aceh, Indonesia*

Email: muhammad.237410101013@mhs.unimal.ac.id, Nora.237410101021@mhs.unimal.ac.id, Cut.237410101034@mhs.unimal.ac.id, Zulfadly.237410101006@mhs.unimal.ac.id, Nurfahni.237410101025@mhs.unimal.ac.id, malahayati@unimal.ac.id, muhammad.hatta@unimal.ac.id

Citation: G. Muhammad, L. Nora, A. Cut, S, Zulfadly, N. Nurfahni, M. Malahayati, H. Muhammad, "Kejahatan Mayantara (Cyber Crime) dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI)," Cendekia: Jurnal Hukum, Sosial & Humaniora, 2, no. 3 (2024): 797-809.

Received: 05 Agustus 2024
Revised: 01 September 2024
Accepted: 22 September 2024
Published: 09 Oktober 2024

**Corresponding Author: muhammad.237410101013@mhs.unimal.ac.id*

Abstrak: Penelitian ini mengkaji tentang respons sistem peradilan pidana terhadap tindak pidana peretasan sistem Bank Syariah Indonesia (BSI) dan mengidentifikasi strategi potensial untuk meningkatkan perlindungan hukum terhadap perbankan di Indonesia. Penelitian ini merupakan penelitian normatif dengan menggunakan pendekatan undang-undang. Hasil penelitian ini menunjukan bahwa peretasan secara illegal diatur dalam Pasal 30 ayat (1), (2), dan (3) Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menentukan bahwa akses tidak sah terhadap sistem elektronik orang lain merupakan pelanggaran hukum. Dalam penanggulangan kejahatan mayantara, pemerintah telah membentuk Badan Siber dan Sandi Negara (BSSN) sebagai lembaga khusus dan independen. Berdasarkan Peraturan Presiden Nomor 133 Tahun 2017 tentang Badan Siber dan Sandi Negara menentukan bahwa BSSN bertanggung jawab melaksanakan upaya keamanan siber secara efektif dan efisien melalui pemanfaatan, pengembangan, dan koordinasi seluruh aspek keamanan siber nasional.

Kata Kunci: *Kejahatan Siber; Implikasi Hukumnya; Peretasan; BSI*

Abstract: *This study investigated the response of the criminal justice system to the hacking of the Bank Syariah Indonesia (BSI) system and identified potential strategies to strengthen the legal protection of banks in Indonesia. This study used a normative approach and was conducted using a statutory framework. The findings highlight that unauthorized access to an individual's electronic system is prohibited by Article 30 Paragraphs (1), (2), and (3) of Law No. 19 of 2016 concerning Electronic Information and Transactions. To combat cybercrime, the government established the National Cyber and Crypto Agency (BSSN) as a specialized and independent organization. Presidential Regulation No. 133/2017 on the National Cyber and Crypto Agency mandates that BSSN is responsible for effectively and efficiently implementing cyber security*

measures by using, developing and coordinating all aspects of national cyber security.

Keywords: *Cyber Crime; Legal Implications; Hacking; BSI*

1. PENDAHULUAN

Pesatnya kemajuan teknologi di era digital saat ini, teknologi informasi telah menjadi komponen yang sangat penting baik dalam kehidupan kita sehari-hari maupun dalam dunia bisnis. Meskipun evolusi teknologi ini tidak diragukan lagi membawa banyak keuntungan, hal ini juga membuka jalan bagi munculnya bentuk-bentuk aktivitas kriminal baru, seperti kejahatan dunia maya atau kejahatan siber.[1]

Cybercrime mengacu pada aktivitas kriminal yang dilakukan dengan menggunakan teknologi komputer atau data digital, khususnya di bidang perbankan yang mana informasi pribadi individu menjadi sasaran dan disusupi.[2] Jenis kejahatan ini mencakup berbagai perilaku terlarang yang dilakukan secara online, seperti akses tidak sah ke sistem komputer, mencuri informasi sensitif, menyebarkan perangkat lunak berbahaya, dan banyak lagi.[3] Berdasarkan informasi Kominfo, Indonesia menempati peringkat ketiga negara dengan jumlah kasus kejahatan siber tertinggi secara global, setelah Ukraina. Penting untuk secara konsisten memprioritaskan kesadaran akan statistik yang mengkhawatirkan ini.[4]

Pada tanggal 14 Mei 2023, Bank Syariah Indonesia (BSI) menjadi korban serangan kejahatan dunia maya ketika peretas membobol data penting mereka. Pelanggaran ini mengakibatkan gangguan bagi bank karena mereka menjadi sasaran serangan ransomware. Ransomware adalah perangkat lunak berbahaya yang digunakan peretas untuk mengenkripsi data dan memblokir akses ke sistem komputer korban hingga uang tebusan dibayarkan. Para peretas di balik serangan ini meminta bank menghubungi mereka dalam waktu 72 jam, mengancam akan menghancurkan reputasi bank jika tuntutan mereka tidak dipenuhi.[5]

Teguh Aprianto, pengamat dunia maya, melalui akun Twitter-nya mengungkapkan bahwa sekelompok peretas secara sistematis membocorkan data BSI. Informasi yang bocor berjumlah 8.133 file, meliputi data pribadi 24.437 pegawai BSI dan dokumen internal. Informasi yang dibobol adalah nomor ponsel, alamat email, alamat rumah, nomor ID karyawan, jabatan, informasi departemen, dan rincian manajer yang bertanggung jawab. Pelanggaran ini juga berdampak pada mantan karyawan, sehingga membahayakan data

---

1 D. Solak and M. Topaloglu, "The Perception Analysis of Cyber Crimes in View of Computer Science Students," *Procedia - Social and Behavioral Sciences* 182 (n.d.): 590–595, https://doi.org/10.1016/j.sbspro.2015.04.787.

2 Doris Karina and Oropeza Mendoza, "The Vulnerability of Cyberspace - The Cyber Crime," *Journal of Forensic Sciences & Criminal Investigation* 2, no. 1 (2017): 1–8.

3 Irma Nurrizki Rahmawati and others, 'Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah', *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora*, 3.2 (2023), 208–15.

4 F Muin, 'Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi', *IDRIS: InDonesian Journal of Islamic Studies*, 1.1 (2023), 97–113.

5 Nicky Maulana et al., "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah," *Inovative: Journal Of Social Science Research* 4 (2024): 8244–58.

pribadi mereka.[6] Kehadiran ancaman ini melemahkan landasan kepercayaan dan membahayakan komitmen Bank dalam menjaga kerahasiaan.

Pernyataan tersebut sangat kontras dengan pernyataan publik yang dikeluarkan Bank BSI. Masalah seputar pemeliharaan sistem yang diangkat secara langsung bertentangan dengan pengungkapan signifikan yang dibuat oleh kepala lembaga penelitian keamanan siber CISSReC, yang mengonfirmasi bahwa bank tersebut memang menjadi korban serangan ransomware. Pelanggaran ini tidak hanya menimbulkan kekhawatiran mengenai kemampuan bank untuk melindungi informasi pribadi yang sensitif tetapi juga melanggar peraturan yang diuraikan dalam Pasal 46 Undang-Undang Perlindungan Data Pribadi.[7] Menurut pasal ini, jika terjadi pelanggaran data, pihak yang terkena dampak wajib memberikan pemberitahuan tertulis dalam waktu 72 jam.[8] Kekurangan ini harus diatasi karena sejalan dengan meningkatnya prevalensi digitalisasi. Kegagalan dalam mengatasi masalah ini dapat menimbulkan dampak buruk bagi perbankan di Indonesia, khususnya Bank BSI, dan masyarakat luas akibat meluasnya adopsi transaksi non-tunai di era digital saat ini.

Penting bagi setiap individu untuk memiliki perlindungan hukum untuk melindungi data pribadi mereka, dan merupakan tugas negara untuk memastikan bahwa hak-hak dasar ini ditegakkan. Sebagaimana tercantum dalam Pasal 28 G ayat (1): "Setiap orang berhak atas perlindungan informasi pribadi, keluarga, nama baik, martabat, dan harta benda yang dikuasainya, serta berhak atas rasa aman dan terlindungi dari ketakutan akan potensi kerugian atau pelanggaran." Hal ini menyoroti pentingnya memastikan bahwa data pribadi disimpan dengan aman, dan bahwa individu dapat percaya bahwa informasi mereka akan dilindungi dari penyalahgunaan atau akses tidak sah. Penting bagi pembuat kebijakan untuk memprioritaskan penerapan dan penegakan hukum yang menjaga privasi pribadi dan perlindungan data.[9]

Menyadari pentingnya peran operasional perbankan dalam mendorong pertumbuhan bangsa, pemerintah telah menetapkan peraturan untuk mengawasi seluruh aktivitas perbankan. Namun penegakan peraturan tersebut di masyarakat seringkali tidak sesuai harapan. Kesenjangan antara standar ideal dan praktik nyata menunjukkan perlunya pertimbangan yang cermat terhadap prinsip-prinsip seperti kerahasiaan bank dan perlindungan data pribadi, serta memastikan kepatuhan terhadap undang-undang dan peraturan terkait.

2. METODE PENELITIAN

Metodologi yang digunakan dalam tulisan ini adalah teknik penelitian hukum normatif dengan menggunakan pendekatan peraturan perundang-undangan (*Statute Approach*)

---

6 Trianda Lestari, "Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi Nasabah Akibat Peretasan Studi Kasus Bank Syariah Indonesia," *Jurnal Perbankan* 2, no. 3 (2024): 48–59.

7 Dewa Gede Sudika Mangku et al., "The Personal Data Protection of Internet Users in Indonesia," *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 203–9, https://doi.org/https://doi.org/10.35741/issn.0258-2724.56.1.23.

8 Yoannisa Fitrian Suhayati, Azri Nur Maulina, and Widwi Handari Adji , 'Pengaruh Pemahaman Bertransaksi Menggunakan Webform BSI Dan BSI Mobile Terhadap Kepuasan Nasabah', *Al-Kharaj : Jurnal Ekonomi, Keuangan & Bisnis Syariah*, 4.6 (2022), 1681–95.

9 Rosihan Luthfi, 'Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia', Jurnal Sosial Teknologi, 2.5 (2022), 431–36.

khususnya yang berkaitan dengan peraturan perundang-undangan perbankan dan Undang-Undang Informasi Dan Transaksi Elektronik. Penelitian hukum normatif adalah proses sistematis untuk mengungkap berbagai aturan, prinsip, asas hukum, menganalisis kekaburan hukum, sejarah hukum dan doktrin hukum untuk mengatasi tantangan hukum.[10]

Penelitian ini memanfaatkan berbagai bahan hukum sekunder sebagai sumber data utama dalam penelitian ini. Data sekunder yang dimaksud dalam penelitian ini berupa peraturan perundang-undangan, putusan pengadilan, risalah hukum, jurnal ilmiah hukum, literatur hukum, dan sumber data hukum secara online.[11] Proses pengumpulan data dilakukan dengan melakukan tinjauan kepustakaan secara menyeluruh terhadap literatur yang terkait dengan objek penelitian ini dan data yang dikumpulkan akan dianalisis menggunakan metode deskriptif kualitatif.

3. HASIL DAN PEMBAHASAN

3.1. Penegakan Hukum Terhadap Tindak Pidana Peretasan Bank Syariah Indonesia

Pesatnya kemajuan teknologi telah melahirkan kejahatan siber (*cybercrime*) yang mempunyai dampak positif dan negatif.[12] Pada satu sisi, teknologi telah memungkinkan komunikasi yang nyaman melalui email dan transaksi keuangan yang efisien melalui internet banking.[13] Sisi lain, teknologi yang sama juga membuka jalan bagi aktivitas kriminal seperti peretasan, di mana individu mengeksploitasi kerentanan dalam sistem untuk mencuri informasi sensitif.[14] Dampak negatif ini menyoroti pentingnya menjaga langkah-langkah keamanan siber yang kuat di era digital.[15]

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memuat ketentuan yang mengatur tindak pidana peretasan pada pasal 30 ayat (1), (2), dan (3). Berdasarkan ketentuan tersebut, individu yang secara melawan hukum berupaya menyusup atau mendapatkan akses terhadap sistem elektronik orang lain akan dianggap melanggar hukum. Lebih lanjut, pasal 46 ayat (1), (2), dan (3) UU ITE menguraikan sanksi pidana bagi mereka yang terbukti melakukan pelanggaran sebagaimana dimaksud dalam pasal 30. Kedua pasal ini bekerja sama untuk memastikan bahwa individu yang terlibat dalam aktivitas peretasan bertanggung jawab atas tindakan mereka.[16]

Dalam hal penegakan hukum, khususnya di bidang kejahatan dunia maya, jenis pelanggaran ini mempunyai dampak luas yang melampaui batas negara dan

---

[10] Yati Nurhayati, Ifrani Ifrani, and M. Yasir Said, 'Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum', *Jurnal Penegakan Hukum Indonesia*, 2.1 (2021), 1–20.

[11] Theresia Anita Christiani, "Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object," *Procedia-Social and Behavioral Sciences* 219 (2016): 201–7, https://doi.org/http://dx.doi.org/10.1016/j.sbspro.2016.05.006.

[12] Johari, "Kedudukan Asas Legalitas Dalam Pembaharuan Hukum Pidana Di Indonesia," *Cendekia : Jurnal Hukum, Sosial Dan Humaniora* 1, no. 1 (2023): 65–77, https://doi.org/https://journal.lps2h.com/cendekia/article/view/11.

[13] Raul Bernardino, "Cyber Crime" (Kupang, 2017).

[14] Muhammad Hatta, "Efforts to Overcome Cyber Crime Actions in Indonesia," *International Journal of Psychosocial Rehabilitation* 24, no. 3 (2020): 1761–68, https://doi.org/10.37200/IJPR/V24I3/PR200925.

[15] Raodia Raodia, 'Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)', *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, 6.2 (2019), 39.

[16] Hukum Perusahaan and D A N Etika, "Jurnal Hukum Progresif:" XI, no. 2 (2017): 1928–40.

menjadikannya isu transnasional. Tanpa kolaborasi antar negara untuk memerangi dan menegakkan hukum terhadap kejahatan transnasional, permasalahan yurisdiksi dapat muncul. Hukum internasional menguraikan berbagai prinsip, seperti prinsip teritorial, kebangsaan, perlindungan, dan universal, yang dapat diterapkan untuk menentukan yurisdiksi dalam kasus-kasus tersebut.[17]

a. Prinsip teritorial: Prinsip ini dianggap sebagai landasan dan landasan perkara yurisdiksi, karena prinsip ini menetapkan kewenangan negara atas segala hal yang terjadi di dalam wilayahnya. Konsep dasar itulah yang menentukan hak negara untuk mengatur dan mengadili setiap dan seluruh kejadian di dalam batas wilayahnya.
b. Prinsip nasionalitas: Berdasarkan prinsip ini, pemerintah diberikan kewenangan untuk mengadili setiap orang atas tindak pidana yang dilakukannya, di mana pun orang tersebut berada. Artinya, negara mempunyai kewenangan untuk melakukan tindakan hukum terhadap warga negaranya di mana pun mereka berada.
c. Prinsip perlindungan: Prinsip ini berfokus pada menjaga kepentingan penting negara, memastikan keamanan dan kesejahteraan negara diprioritaskan di atas segalanya.
d. Prinsip universal: Prinsip ini berlaku dalam berbagai konteks dan secara umum diakui oleh masyarakat. Dalam kerangka hukum ini, setiap negara diberikan kewenangan untuk mengadili pelanggaran tertentu yang menimbulkan ancaman bagi masyarakat dalam skala global.

Salah satu metode bagi suatu negara untuk menegaskan otoritasnya atas seorang penjahat di yurisdiksi asing adalah dengan meminta penangkapan pelaku dari negara tempat mereka berada. Dalam kasus kejahatan dunia maya, khususnya peretasan, yurisdiksi dapat dibentuk melalui upaya kolaboratif antar negara, seperti ekstradisi, bantuan hukum timbal balik, dan kerja sama antar lembaga penegak hukum. Melalui cara-cara ini, negara-negara dapat bekerja sama untuk mengatasi dan mengadili penjahat dunia maya yang beroperasi lintas batas negara.[18]

Dalam menangani kejahatan dunia maya seperti peretasan, upaya penegakan hukum dapat diperkuat dengan meningkatkan kesadaran masyarakat. Berbeda dengan kejahatan tradisional seperti pembunuhan atau pemerkosaan, kejahatan dunia maya memerlukan alat dan keahlian teknologi khusus untuk penyelidikan dan penuntutan. Dengan mengedukasi masyarakat tentang prevalensi dan konsekuensi kejahatan dunia maya, kita dapat memberdayakan individu untuk berperan proaktif dalam mencegah dan melaporkan aktivitas ilegal tersebut.

Salah satu kasus kejahatan siber di Indonesia adalah perentasan sistem Bank Syariah Indonesia (BSI).[19] Bank BSI, bank yang beroperasi terutama secara online, telah menjadi sasaran utama aktivitas kriminal, khususnya di bidang kejahatan dunia maya. Peretasan data nasabah telah menjadi masalah yang menonjol bagi Bank BSI, sehingga mendorong perhatian lebih dekat terhadap legalitas tindakan tersebut dan tindakan yang diperlukan untuk melindungi informasi nasabah dari ancaman dunia maya. Penelitian ini akan

---

[17] Nabillah Kamila Affandi and Ayu Nrangwesti, "Hukum Laut Internasional." *Armed Piracy Law Enforcement in the Malacca Strait Under the International Law of the Sea* 5, no. 1 (2023): 82–93.

[18] Galuh Kartiko, "Pengaturan Terhadap Yurisdiksi," *Trunojoyo*, 2017, 1–18.

[19] Zahra Fatikhatun Nisa and Yuli Tri Cahyono, "The Effect of Cyber Attacks on Stock Performance Bank Syariah Indonesia," *Proceeding International Conference on Accounting and Finance* 2 (2024): 359–368, https://doi.org/https://journal.uii.ac.id/inCAF/article/view/32669.

menyelidiki seluk-beluk kejahatan dunia maya, khususnya berfokus pada peretasan data nasabah Bank BSI, dan mengeksplorasi solusi potensial untuk meningkatkan keamanan data. Berdasarkan artikel di Kompas.com, Bareskrim Dittipidisiber Polri telah memulai penyelidikan menyeluruh atas insiden peretasan dan dugaan pembobolan data yang terjadi di BSI. Pelaku, yang diidentifikasi sebagai kelompok pengembangan perangkat lunak LockBit, berhasil menyusup ke sistem BSI, menimbulkan kekhawatiran tentang keamanan informasi sensitif. Pihak berwenang bekerja keras untuk mengungkap sepenuhnya pelanggaran tersebut dan memastikan bahwa mereka yang bertanggung jawab bertanggung jawab atas tindakan mereka.[20]

Sebelum menjadi sasaran serangan peretasan pada 8 Mei 2023, sistem BSI sudah mengalami kegagalan fungsi. Dalam sistem perbankan, terdapat banyak sekali data sensitif seperti alamat, saldo rekening, riwayat transaksi, tanggal pembukaan rekening, rincian pekerjaan, dan sejumlah informasi lainnya yang akhirnya disusupi. Data klien yang bocor mencakup detail pribadi seperti nama, nomor telepon, alamat, modifikasi akun, aktivitas perdagangan, tanggal dimulainya akun, catatan pekerjaan, dan sejumlah data lainnya.

Tahapan atau rangkaian kronologi peretasan BSI:[21]

a. Senin, 8 Mei 2023: Platform digital BSI, termasuk ATM dan Aplikasi BSI Mobile, saat ini tidak tersedia karena sedang dilakukan pemeliharaan oleh pihak bank.
b. Selasa, 9 Mei 2023: BSI mengeluarkan pernyataan bahwa pemulihan layanan ATM akan dilakukan secara bertahap dengan pemantauan terus menerus oleh Sekretaris Perusahaan Gunawan Arief Hartoyo. Sementara itu, aplikasi BSI Mobile tetap tidak dapat diakses karena terkadang dapat dibuka namun tidak dapat menyelesaikan transaksi. Perusahaan secara aktif berupaya mengatasi masalah ini dan memberikan pembaruan bila diperlukan.
c. Rabu, 10 Mei 2023: Penyebaran ransomware semakin mengkhawatirkan karena penyebab gangguan tersebut masih belum jelas dan belum ada pernyataan resmi yang dikeluarkan oleh BSI. Dilumpuhkannya layanan digital BSI berdampak besar pada provinsi Aceh yang sudah menerapkan sistem keuangan syariah. BSI merupakan pelaku pasar terbesar kedua setelah Bank Aceh, dan gangguan ini juga berdampak pada pembayaran biaya haji.
d. Kamis, 11 Mei 2023: Dalam jumpa pers sore harinya, Direktur Utama BSI Hery Gunardi mengumumkan layanan digital sudah kembali beroperasi normal meski bertahap. Gunardi menyebutkan adanya potensi tanda-tanda serangan siber yang berujung pada penutupan sementara sistem. Namun, dia menegaskan tuduhan tersebut harus dibuktikan kebenarannya. BSI bekerja sama dengan beberapa entitas, termasuk Bank Mandiri, Bank Indonesia, dan Otoritas Jasa Keuangan, untuk mempercepat proses pemulihan sistem.
e. Jumat, 12 Mei 2023: Hari terakhir jamaah haji melakukan pembayaran biaya haji, BSI melaporkan 95 persen jamaah sudah menyerahkan setoran. Untuk membantu mereka

[20] George Anderson Tirta and Gunardi Lie, 'Tinjauan Hukum Terhadap Tindak Pidana Cybercrime Dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI)', *MANTAP: Journal of Management Accounting, Tax and Production*, 2.1 (2024), 240–49.

[21] Maulana et al., "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah."

yang belum menyelesaikan pembayarannya, BSI mengumumkan rencana pembukaan 434 cabang selama akhir pekan. Selain itu, layanan dan fungsi digital BSI Mobile terus meningkat.

f. Sabtu, 13 Mei 2023: LockBit 3.0, kelompok peretas ransomware terkenal, telah mengumumkan bahwa mereka berhasil melancarkan serangan terhadap BSI dan berhasil memperoleh 1,5 TB data pribadi dari server organisasi. Para peretas menetapkan batas waktu hingga 15 Mei 2023 bagi BSI untuk membayar uang tebusan guna mencegah data bocor ke publik. Meskipun situasi ini serius, BSI tetap bungkam dan belum mengeluarkan pernyataan resmi apa pun sebagai tanggapan atas klaim yang dibuat oleh LockBit 3.0.

g. Ahad-Senin, 14-15 Mei 2023: Layanan BSI saat ini sedang dalam proses pemulihan dan sebagian besar fungsinya berjalan seperti biasa. Batas waktu untuk LockBit 3.0 telah berlalu.

h. Selasa, 16 Mei 2023: Ada kecurigaan bahwa LockBit 3.0 telah mendistribusikan data yang dicurinya di web gelap. Informasi yang diambil terbanyak adalah pada 8 Mei 2023. Saham BRIS kembali mengalami kenaikan nilainya. BSI telah merilis pernyataan yang menyangkal adanya pelanggaran keamanan dan memastikan pelanggan bahwa data dan dana mereka aman.

i. Sabtu, 20 Mei 2023: Investigasi serangan siber terhadap Bank Syariah Indonesia (BSI) telah dimulai dan dilakukan secara menyeluruh oleh Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim Polri). Bareskrim Polri bekerja sama dengan berbagai pihak terkait, termasuk Badan Siber dan Sandi Negara (BSSN), untuk mengusut lebih dalam kejadian serangan siber tersebut.

Demi menjaga hak subjek data, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengamanatkan organisasi untuk mematuhi berbagai peraturan, antara lain Peraturan OJK, Peraturan Pemerintah No. 71 Tahun 2019 tentang Sistem dan Transisi Elektronik (PP PSTE), dan Permenkominfo no. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo PDPSE). Sesuai dengan peraturan ini, BSI diwajibkan untuk segera memberi tahu pelanggan mengenai pelanggaran apa pun dalam perlindungan data pribadi, memberikan perincian tentang data yang disusupi, waktu dan cara pelanggaran, serta langkah-langkah yang diambil untuk mengatasi dan memulihkan insiden tersebut.[22]

Implikasi hukum seputar peretasan data Bank BSI menjadi kerangka penegakan konsekuensi terhadap individu yang melakukan aktivitas kriminal. Berdasarkan Pasal 36 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, pelanggar dapat dikenakan sanksi seperti teguran lisan atau tertulis, penghentian kegiatan, dan pengumuman publik di platform online. Aturan ini berakar pada asas yang tertuang dalam ayat awal Pasal 26 Undang-Undang No. 19 Tahun 2016. Undang-undang sangat penting untuk memberikan efek jera dan memberikan pedoman dalam mengatasi perilaku terlarang demi menjaga ketertiban dan menegakkan keadilan dalam

[22] Muhammad Yudistira and Ramadhan, 'Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo', *Unes Law Review*, 5.4 (2023), 3802–15.

masyarakat.[23] Sesuai ketentuan yang mengharuskan adanya persetujuan seseorang sebelum memanfaatkan data pribadinya secara elektronik, maka peristiwa peretasan dalam kasus Bank BSI termasuk pencurian berdasarkan Pasal 362 KUHP. Pelanggaran ini mencakup unsur obyektif dan subyektif, dan penanganannya telah berkembang berdasarkan sifat kegiatannya. Selain itu, tercatat telah terjadi peretasan terhadap pengguna Bank BSI yang melanggar Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini, khususnya Pasal 30, 46, dan 52, mengatur setiap akses tidak sah yang disengaja ke komputer atau perangkat elektronik dan menguraikan sanksi terkait atas tindakan tersebut.[24]

Total terdapat 19 tindak pidana berbeda yang dituangkan dalam Pasal 27 hingga Pasal 37 UU ITE. Salah satu pelanggaran tersebut adalah pencurian bank melalui ATM, serupa dengan pencurian uang tunai melalui platform digital seperti web office. Tindakan ini dianggap serupa dengan membobol sistem yang aman untuk mengakses properti secara tidak sah, sehingga mengakibatkan kerugian finansial bagi orang lain. Konsep merugikan orang lain melalui kegiatan ilegal tersebut merupakan aspek krusial dalam delik ITE sebagaimana tercantum dalam Pasal 30 Ayat (3). Konsep menimbulkan kerugian ini juga diatur dalam Pasal 36 undang-undang tersebut.[25]

Dalam Kitab Undang-Undang Hukum Pidana (KUHP) memuat ketentuan yang dapat diterapkan untuk mengadili kejahatan siber melalui penafsiran yang luas, antara lain ketentuan terkait pemalsuan (Pasal 263 hingga 276), pencurian (Pasal 362 hingga 367), penipuan (Pasal 378 hingga 395), dan pengrusakan harta benda (Pasal 378 hingga 395). 407 hingga 412). Dalam kasus pencurian informasi pribadi nasabah di industri perbankan, undang-undang dalam KUHP, seperti terkait phishing, juga dapat digunakan untuk penuntutan.

3.2. Perlindungan Hukum Terhadap Sistem Perbankan di Indonesia dari Serangan Kejahatan Siber

Upaya untuk memerangi kejahatan dunia maya melibatkan peningkatan kesadaran masyarakat tentang pentingnya keamanan dunia maya, mendidik individu tentang praktik online yang aman, dan mengembangkan lingkungan yang mendukung langkah-langkah keamanan dunia maya. Selain itu, pemerintah ditugaskan untuk menawarkan sumber daya dan program pelatihan untuk membekali masyarakat umum dan profesional TI dengan keterampilan yang diperlukan untuk melindungi diri dari ancaman dunia maya. Kunci untuk secara efektif memerangi gelombang ancaman siber terletak pada kerja sama antara lembaga pemerintah dan sektor swasta, khususnya di industri seperti perbankan.

Selain itu, sangat penting bagi masyarakat umum untuk berhati-hati dan tetap waspada terhadap kejahatan dunia maya, serta mendidik satu sama lain tentang potensi

---

[23] Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *UU No. 19 Tahun 2016*, no. 1 (2016): 1–31.

[24] Tonny Rompi and Harly Stanly Muaja, 'Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan', *Lex Privatum*, 9.4 (2021), 183–92.

[25] Jeremy Samuel Pangkey Sondakh, Harly Stanly Muaja, and Fonny Tawas, "Pemberlakuan Ketentuan Pidana Dalam Pasal 27 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Lex Privatum* 9, no. 5 (2021): 86–93.

konsekuensi jika menjadi korban dari aktivitas jahat ini. Dengan bekerja sama dan tetap berhati-hati, kita dapat meminimalkan dampak negatif kejahatan dunia maya terhadap masyarakat kita.[26] Pendekatan yang dilakukan BSSN dalam mendorong keamanan siber di Indonesia berkisar pada lima pilar yang dituangkan dalam laporan GCI 2017, dengan fokus pada Aspek Hukum. Pilar ini mengevaluasi keberadaan institusi dan kerangka hukum terkait keamanan siber dan kejahatan siber.

Aspek teknis dinilai dengan memeriksa ketersediaan lembaga teknis dan kerangka kerja yang didedikasikan untuk meningkatkan langkah-langkah keamanan siber. Evaluasi aspek organisasi mencakup penilaian apakah terdapat lembaga khusus di tingkat nasional yang bertanggung jawab untuk mengoordinasikan kebijakan dan strategi pengembangan keamanan siber. Dalam hal pengembangan kapasitas, fokusnya adalah pada adanya inisiatif penelitian dan pengembangan. Terakhir, aspek kolaborasi dievaluasi dengan melihat adanya kemitraan di bidang keamanan siber.[27]

Penguatan keamanan dan ketahanan siber yang diwujudkan dengan strategi berikut:[28]

a. Meningkatkan keamanan infrastruktur siber sangat penting di era digital saat ini.;
b. Peningkatan dan perluasan Computer Emergency Response Team (CERT) melalui berbagai inisiatif dan strategi yang bertujuan untuk meningkatkan kemampuannya dalam merespons insiden dan ancaman keamanan siber.
c. Pencegahan kejahatan siber dan peningkatan kerja sama global di bidang keamanan siber merupakan komponen penting dalam melindungi individu, organisasi, dan negara dari meningkatnya ancaman aktivitas online yang berbahaya.;
d. Meningkatkan keterampilan dan keahlian individu di bidang keamanan siber untuk lebih melindungi aset dan data digital dari potensi ancaman dan pelanggaran; dan
e. Tingkat penyelesaian kejahatan dunia maya melalui penyelesaian atau penuntutan dalam sistem hukum.

Dalam upaya untuk mendukung upaya global dalam meningkatkan keamanan siber, Persatuan Telekomunikasi Internasional (ITU) telah melakukan penilaian melalui Indeks Keamanan Siber Global (GCI) untuk seluruh 193 negara anggota. Pemeringkatan GCI terbaru tahun 2020 menempatkan Indonesia pada posisi ke-77. Namun, laporan tersebut menyoroti fakta yang mengkhawatirkan bahwa kemajuan Indonesia dalam mengembangkan kebijakan keamanan siber masih berada di angka 0%, terutama mengingat meningkatnya jumlah serangan siber yang menargetkan negara ini selama lima tahun terakhir. Upaya yang bisa dilakuan diantaranya:[29]

a. Pelatihan dan peningkatan keterampilan keamanan siber dilakukan secara kolaborasi, pembenahan mekanisme pertahanan sesuai dengan protokol pertahanan siber dan keamanan siber.

---

[26] Rinitami Njatrijani, "Law , Development & Justice Review Law , Development & Justice Review," *Law, Development & Justice Review* 3, no. 2 (2022): 1–9.

[27] Yusep Ginanjar, 'Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara', *Jurnal Dinamika Global*, 7.02 (2022), 291–312.

[28] Ginanjar.

[29] Diny Luthfah, 'Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia', *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, 9 (2023), 259–67.

b. Pembentukan Undang-Undang Khusus tentang Tindak Pidana Siber. Dimana Peraturan perundang-undangan di bidang teknologi informasi yang berlaku di Indonesia saat ini belum mengakomodir seluruh tindak pidana siber, sehingga terdapat beberapa kejahatan siber yang saat ini menjadi persoalan terhadap keamanan dan pertahanan (sebagai faktor dalam menjaga keamanan dan kedaulatan negara) belum diatur dalam regulasi nasional.

c. Peningkatan Sumberdaya Manusia Peran sumber daya manusia sangat penting dalam menegakkan langkah-langkah keamanan siber secara efektif sejalan dengan protokol yang telah ditetapkan.

d. Untuk mengatasi kebutuhan keamanan yang terus berkembang secara efektif, individu harus memiliki dan terus memperbarui pengetahuan dan keterampilan khusus mereka. Berkolaborasi dengan berbagai pemangku kepentingan di dalam negeri melalui pendekatan multi-pemangku kepentingan sangat penting dalam meningkatkan langkah-langkah keamanan dalam negeri.

e. Meningkatkan kolaborasi global dalam kemajuan dan penguatan kemampuan keamanan siber sangat penting untuk memperkuat infrastruktur dan sumber daya di bidang keamanan siber. Hal ini mencakup pengembangan dan perluasan kapasitas kemampuan keamanan siber dalam skala global, baik dari segi infrastruktur maupun sumber daya.

Peraturan Nomor 11/POJK.03/2022 atau dikenal dengan POJK PTI yang diterbitkan Otoritas Jasa Keuangan fokus pada pemanfaatan teknologi informasi oleh bank umum. Hal ini mencakup pedoman mengenai ketahanan siber dan langkah-langkah keamanan yang harus diterapkan oleh bank-bank tersebut. Peraturan ini dijabarkan lebih lanjut dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

a. Proses Identifikasi Aset, Ancaman, dan Kerentanan Bank memanfaatkan manajemen aset dengan melakukan inventarisasi dan penilaian menyeluruh terhadap aset TI yang mencakup perangkat keras, perangkat lunak, sumber daya manusia, jaringan, dan infrastruktur. Hal ini juga memastikan bahwa konfigurasi dicatat dan dipelihara secara akurat untuk mengoptimalkan efisiensi dan efektivitas.

b. Proses Deteksi Insiden Siber, Bank berkomitmen untuk memelihara dokumentasi kinerja yang komprehensif untuk fungsi-fungsi penting dan sistem pendukungnya untuk memastikan bahwa setiap penyimpangan dapat segera diidentifikasi dan setiap aktivitas atau kejadian mencurigakan segera dilaporkan untuk penyelidikan lebih lanjut. Dokumentasi ini berfungsi sebagai alat yang berharga dalam memantau operasi Bank dan menjaga terhadap potensi risiko.

Proses Penanggulangan dan Pemulihan Insiden Siber, Bank telah mengembangkan rencana komprehensif untuk merespons dan memulihkan insiden dunia maya guna memulihkan layanan dengan cepat dengan gangguan minimal. Rencana ini dirancang untuk memastikan respons yang cepat dan efisien terhadap setiap insiden dunia maya yang mungkin terjadi, sehingga memungkinkan Bank untuk melanjutkan operasi normal sesegera mungkin sambil meminimalkan dampak negatif apa pun.

4. KESIMPULAN

Berdasarkan hasil analisis yang dilakukan dapat disimpulkan bahwa 3 artikel berita yang wartawan Harian Kompas menggunakan sumber sumber yang relevan. Terlihat pada ke 3 artikel tersebut yang dimana Harian Kompas mencantumkan sumber yang mereka ambil, *Framing* pemberitaan konflik israel-palestina dalam harian *(e-paper)* kompas sendiri cenderung dengan pendekatan yang berimbang dan berdasarkan prinsip-prinsip jurnalisme yang objektif. Harian Kompas menjadi salah satu media terkemuka di Indonesia, biasanya memberikan berita yang keprehensif dan mendalam mengenai konflik tersebut.

Harian Kompas berupaya untuk menyajikan informasi dari berbagai sudut pandang yang berbeda, termasuk pandangan Israel dan Palestina, serta dampak konflik tersebut terhadap masyarakat dan hubungan internasional. Dalam memberitakan Israel-Palestina, Harian Kompas biasanya mengutamkan fakta- fakta yang terverifikasi dan memberikan ruang bagi berbagai pihak untuk menyampaikan pendapat dan pandangan mereka. Selain itu, Harian Kompas juga menghindari penyampaian infromasi yang bepihak atau tendensius, serta mengedepankan prinsip keberimbangan dalam pemberitaan.

Sebagai Media yang bertanggung jawab, jurnalis Harian Kompas juga sering kali menyajikan analisis mendalam mengenai akar masalah konflik Israel-Palestina, perkembangan terkini, serta upaya perdamaian yang dilakukan oleh pihak terkait. Dengan demikian, Harian Kompas berusaha untuk memberikan informasi yang seimbang dan obyektif kepada pembacanya agar dapat membentuk pemahaman yang komprehensif mengenai konflik tersebut.

DAFTAR PUSTAKA

Affandi, Nabillah Kamila, and Ayu Nrangwesti. “Hukum Laut Internasional." *Armed Piracy Law Enforcement in the Malacca Strait Under the International Law of the Sea* 5, no. 1 (2023): 82–93.

Bernardino, Raul. “Cyber Crime.” Kupang, 2017.

Christiani, Theresia Anita. “Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object.” *Procedia-Social and Behavioral Sciences* 219 (2016): 201–7. https://doi.org/http://dx.doi.org/10.1016/j.sbspro.2016.05.006.

D. Solak and M. Topaloglu. “The Perception Analysis of Cyber Crimes in View of Computer Science Students.” *Procedia - Social and Behavioral Sciences* 182 (n.d.): 590–595. https://doi.org/10.1016/j.sbspro.2015.04.787.

Ginanjar, Yusep. “Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara.” *Jurnal Dinamika Global* 7, no. 02 (2022): 291–312. https://doi.org/10.36859/jdg.v7i02.1187.

Hatta, Muhammad. “Efforts to Overcome Cyber Crime Actions in Indonesia.” *International Journal of Psychosocial Rehabilitation* 24, no. 3 (2020): 1761–68. https://doi.org/10.37200/IJPR/V24I3/PR200925.

Indonesia, Republik. “Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.” *UU No. 19 Tahun 2016*, no. 1 (2016): 1–31.

Jeremy Samuel Pangkey Sondakh, Harly Stanly Muaja, and Fonny Tawas. "Pemberlakuan Ketentuan Pidana Dalam Pasal 27 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Lex Privatum* 9, no. 5 (2021): 86–93.

Johari. "Kedudukan Asas Legalitas Dalam Pembaharuan Hukum Pidana Di Indonesia." *Cendekia : Jurnal Hukum, Sosial Dan Humaniora* 1, no. 1 (2023): 65–77. https://doi.org/https://journal.lps2h.com/cendekia/article/view/11.

Karina, Doris, and Oropeza Mendoza. "The Vulnerability of Cyberspace - The Cyber Crime." *Journal of Forensic Sciences & Criminal Investigation* 2, no. 1 (2017): 1–8.

Kartiko, Galuh. "Pengaturan Terhadap Yurisdiksi." *Trunojoyo*, 2017, 1–18.

Lestari, Trianda. "Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi Nasabah Akibat Peretasan Studi Kasus Bank Syariah Indonesia." *Jurnal Perbankan* 2, no. 3 (2024): 48–59.

Luthfah, Diny. "Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia." *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti* 9 (2023): 259–67. https://doi.org/10.25105/pdk.v9i1.18643.

Luthfi, Rosihan. "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia." *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36. https://doi.org/10.59188/jurnalsostech.v2i5.336.

Mangku, Dewa Gede Sudika, Ni Putu Rai Yuliartini, I. Nengah Suastika, and I. Gusti Made Arya Suta Wirawan. "The Personal Data Protection of Internet Users in Indonesia." *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 203–9. https://doi.org/10.35741/issn.0258-2724.56.1.23.

Maulana, Nicky, Tito Laurens, Hadrian Afzal Faiz, and Tria Patrianti. "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah." *INNOVATIVE: Journal Of Social Science Research* 4 (2024): 8244–58.

Muin, F. "Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi." *IDRIS: InDonesian Journal of Islamic Studies* 1, no. 1 (2023): 97–113.

Nisa, Zahra Fatikhatun, and Yuli Tri Cahyono. "The Effect of Cyber Attacks on Stock Performance Bank Syariah Indonesia." *Proceeding International Conference on Accounting and Finance* 2 (2024): 359–368. https://journal.uii.ac.id/inCAF/article/view/32669.

Njatrijani, Rinitami. "Law , Development & Justice Review Law , Development & Justice Review." *Law, Development & Justice Review* 3, no. 2 (2022): 1–9.

Nurhayati, Yati, Ifrani Ifrani, and M. Yasir Said. "Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum." *Jurnal Penegakan Hukum Indonesia* 2, no. 1 (2021): 1–20. https://doi.org/10.51749/jphi.v2i1.14.

Perusahaan, Hukum, and D A N Etika. "Jurnal Hukum Progresif:" XI, no. 2 (2017): 1928–40.

Rahmawati, Irma Nurrizki, Nova Rahmadani, Diyah Rosita Heni, and Sandro Kevin. "Pertanggungjawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah." *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora* 3, no. 2 (2023): 208–15.

Raodia, Raodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019): 39. https://doi.org/10.24252/jurisprudentie.v6i2.11399.

Rompi, Tonny, and Harly Stanly Muaja. "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan." *Lex Privatum* 9, no. 4 (2021): 183–92.

Suhayati, Yoannisa Fitrian, Azri Nur Maulina, and Widwi Handari Adji . "Pengaruh Pemahaman Bertransaksi Menggunakan Webform BSI Dan BSI Mobile Terhadap Kepuasan Nasabah." *Al-Kharaj : Jurnal Ekonomi, Keuangan & Bisnis Syariah* 4, no. 6 (2022): 1681–95. https://doi.org/10.47467/alkharaj.v4i6.1054.

Tirta, George Anderson, and Gunardi Lie. "Tinjauan Hukum Terhadap Tindak Pidana Cybercrime Dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI)." *MANTAP: Journal of Management Accounting, Tax and Production* 2, no. 1 (2024): 240–49. https://doi.org/10.57235/mantap.v2i1.1634.

Yudistira, Muhammad, and Ramadhan. "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo." *Unes Law Review* 5, no. 4 (2023): 3802–15.