CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 9 No 11 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

PENEGAKAN HUKUM DALAM MENANGGULANGI KEJAHATAN SIBER (*CYBER CRIME*) DI ERA DIGITAL

(Studi Kasus Peretasan Data Pengguna Bank BSI)

Rika Armayanti[1], Dhira Ahzara Permata[2], Srikandi Regita Cahyani[3], Bambang Fitrianto[4]
Program Studi Ilmu Hukum, Fakultas Sosial Sains,
Universitas Pembangunan Panca Budi, Medan, Indonesia
Email : rikaarmayanti@gmail.com, bambangfitrianto@dosen.pancabudi.ac.id

ABSTRAK

Penelitian ini membahas pentingnya penegakan hukum dalam menanggulangi *cyber crime* di era digital dan upaya untuk mencegahnya. Metode yang digunakan adalah analisis yuridis normatif untuk mengeksplorasi undang-undang terkait, literatur hukum, dan dokumen relevan. Bank semakin rentan terhadap ancaman seperti peretasan data dan kejahatan dunia maya lainnya, dengan kasus nyata seperti peretasan data yang terjadi pada tahun 2023 pada Bank Syariah Indonesia (BSI). Temuan utama mencakup kompleksitas regulasi yang masih belum memadai untuk mengatasi dinamika *cyber crime* yang cepat berkembang. Indonesia masih menghadapi tantangan dalam menghadapi kejahatan siber yang semakin canggih dan intens. Kesimpulan dari penelitian ini menekankan perlunya pembaharuan hukum yang lebih adaptif dan komprehensif untuk menanggapi ancaman kejahatan siber yang berkembang pesat. Dengan implementasi yang tepat, diharapkan Indonesia dapat meningkatkan efektivitas penanggulangan *cyber crime*, melindungi aset digital, dan meminimalisir dampak negatif terhadap individu, perusahaan, dan negara secara keseluruhan.

Kata Kunci: Hukum, Cyber crime, Bank BSI

ABSTRACT

This research discusses the importance of law enforcement in combating cyber crime in the digital era and efforts to prevent cybercrime. The method used is normative juridical analysis to explore relevant laws, legal literature, and pertinent documents. Banks are becoming increasingly vulnerable to threats such as data breaches and other cybercrimes, with real cases like the data breach that occurred in 2023 at Bank Syariah Indonesia (BSI). The main findings include the complexity of regulations that are still inadequate to address the rapidly evolving dynamics of cyber crime. Indonesia still faces challenges in dealing with increasingly sophisticated and intense cyber crime. The conclusion of this study emphasizes the need for more adaptive and comprehensive legal reforms to address the rapidly evolving threat of cybercrime. With proper implementation, it is hoped that Indonesia can enhance the effectiveness of combating cyber crime, protect

Article History
Received: Desember 2024
Reviewed: Desember 2024
Published: Desember 2024

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 9 No 11 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

digital assets, and minimize negative impacts on individuals, companies, and the country as a whole.
Keywords: *Law, Cyber crime, Bank BSI*

PENDAHULUAN

Dalam beberapa tahun terakhir, perkembangan teknologi informasi dan komunikasi telah mengubah secara drastis cara bisnis perbankan beroperasi. Digitalisasi layanan perbankan, seperti mobile banking dan internet banking, menawarkan kemudahan dan efisiensi bagi pengguna. Namun, di balik kemudahan ini muncul tantangan serius berupa kejahatan siber yang mengancam integritas dan keamanan sistem perbankan.

Perkembangan teknologi digital telah membawa banyak kemudahan dalam berbagai aspek kehidupan, namun juga menghadirkan tantangan baru, terutama dalam bentuk kejahatan siber atau cyber crime. Kejahatan ini mencakup berbagai kegiatan ilegal yang dilakukan melalui media elektronik, seperti peretasan, pencurian data, dan penipuan online. Salah satu kasus yang mencolok adalah peretasan data pengguna Bank BSI, yang menjadi sorotan publik dan menunjukkan betapa rentannya sistem keamanan informasi di era digital.

Pasal 4 UU No. 11 Tahun 2008 yang diubah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menyebutkan bahwa pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan dengan tujuan untuk: [1]

a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
c. meningkatkan efektivitas dan efisiensi pelayanan publik;
d. membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan teknologi informasi se-optimal mungkin dan bertanggung jawab; dan
e. memberikan rasa aman, keadilan dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi.

Melihat rumusan dari Pasal 4 di atas, pemanfaatan teknologi informasi dan transaksi elektronik yang dilakukan oleh orang-orang yang menguasai teknologi sudah tidak sesuai lagi dengan apa yang menjadi harapan dari UU Informasi dan Transaksi Elektronik sebagaimana yang tercantum dalam tujuannya. Kejahatan siber (*cyber crime*) sudah merambah ke seluruh aspek kehidupan masyarakat. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus juga menjadi sarana efektif perbuatan melawan hukum. [2]

Penegakan hukum dalam konteks kejahatan siber memerlukan kerjasama antara berbagai pihak, termasuk pemerintah, lembaga penegak hukum, dan sektor swasta. Di Indonesia, meskipun ada undang-undang terkait informasi dan transaksi elektronik (UU ITE), masih terdapat tantangan dalam penerapan dan penegakan hukum yang efektif. Banyak kasus kejahatan siber yang sulit diusut karena kurangnya bukti yang kuat dan kompleksitas teknologi yang digunakan oleh pelaku.

---

[1] UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diubah dengan UU No. 19 Tahun 2016.
[2] RATULANGI, Christian Henry. Tindak pidana cyber crime dalam kegiatan perbankan. *Lex Privatum*, 2021, 9.5.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 9 No 11 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

Dalam menghadapi tantangan kejahatan siber di era digital, penegakan hukum yang efektif menjadi sangat penting. Kasus peretasan data pengguna Bank BSI merupakan pengingat bahwa semua pihak perlu berperan aktif dalam melindungi data dan informasi, serta menjaga kepercayaan masyarakat terhadap sistem digital. Keterlibatan pemerintah, lembaga penegak hukum, dan sektor swasta dalam menciptakan regulasi yang kuat dan sistem keamanan yang handal adalah langkah krusial untuk menanggulangi kejahatan siber secara efektif. Dengan demikian, rumusan masalah yang diteliti mencakup bagaimana penegakan hukum berfungsi dalam kasus kebocoran data nasabah Bank Syariah Indonesia, serta upaya penegakan hukum yang telah dilakukan untuk memerangi kejahatan siber dan melindungi keamanan data bank dan nasabah.

LANDASAN TEORI

Kejahatan siber, juga dikenal sebagai *cyber crime*, adalah kejahatan yang terjadi di dunia maya yang menyerang aspek keamanan jaringan komputer dan informasi teknologi telekomunikasi. Di era digital saat ini, jelas bahwa kemajuan teknologi dan informasi dapat berdampak negatif. Perkembangan kejahatan siber atau *cyber crime*, yang dapat merugikan masyarakat, dapat menjadi konsekuensi negatif. Meskipun kejahatan tersebut terkait erat dengan hasil dari budaya seseorang, tingkat budaya yang dianut seseorang dan tingkat modernitas dan perkembangan seseorang berkorelasi langsung dengan tingkat kejahatan yang terjadi di negara tersebut. Baik dalam bentuk, karakteristik, dan cara kejahatan tersebut dilakukan. Kemajuan dalam teknologi dan informasi dapat memiliki efek yang positif dan negatif.[3]

Penyalahgunaan teknologi ini dapat menyebabkan tindakan pidana yang dikenal sebagai "kejahatan dunia siber" atau "kejahatan siber", yang memiliki karakteristik dan ciri-ciri yang berbeda dan terkait dengan jaringan internet dan teknologi. Penanganan kasus kejahatan ini berbeda dari penanganan kasus kejahatan biasa.

Kejahatan di dunia maya menurut peraturan perundang-undangan kerap dihubungkan dengan kejahatan tindak pidana yang memiliki hubungan erat dengan teknologi informasi. Kejahatan dunia maya adalah kejahatan dan tindak pidana yang secara ilegal dan tidak sah menggunakan jaringan informasi dan teknologi tersebut.

Pihak-pihak yang berniat melakukan kejahatan sering mengincar transaksi di bisnis perbankan. Data pelanggan akan disadap dan semua detailnya akan dikumpulkan hingga digunakan untuk tujuan yang tidak menyenangkan. seperti penipuan dan pendanaan teroris. Jika para korban melaporkan kejahatan siber, penyelidikan akan dilakukan. Proses penyidikan didefinisikan sebagai kumpulan penyidik yang bekerja sama untuk mengumpulkan bukti yang kuat agar pelaku dapat ditangkap dan dihukum sesuai dengan undang-undang.

METODE PENELITIAN

Metode yang digunakan adalah hukum normatif (yuridis normatif) yaitu dengan menggunakan pendekatan peraturan perundang-undangan yang berkaitan dengan peraturan perundang-undangan perbankan dan Undang-Undang Informasi Dan Transaksi Elektronik. Penelitian hukum normatif adalah jenis penelitian hukum yang berpusat pada peraturan hukum yang berlaku dan relevan dengan masalah hukum yang dibahas.

[3] Ningrum, Delvyan Putri Surya, and Jamiatur Robekha. "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia." *Journal Evidence Of Law* 1.1 (2022): 112-128.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 9 No 11 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

HASIL DAN PEMBAHASAN

1. Penegakan Hukum Terhadap Tindak Pidana Peretasan Data Pengguna Bank Syariah Indonesia

Pada 8 Mei 2023, serangan siber menyebabkan layanan digital Bank Syariah Indonesia (BSI) mengalami gangguan atau eror selama beberapa hari. Nasabah mengatakan bahwa mereka menghadapi kesulitan saat menggunakan layanan seperti transaksi melalui aplikasi BSI Mobile, ATM, dan teller. Peristiwa kronologi peretasan data nasabah Bank Syariah Indonesia (BSI) yang diuraikan oleh pakar keamanan siber Alfons Tanujaya, terungkap bahwa BSI menjadi sasaran serangan ransomware, khususnya jenis Lockbit. Alfons memaparkan detail peristiwa mulai dari penemuan kebocoran data sebesar 1,5 TB hingga analisis waktu pencurian yang menunjukkan serangan yang terorganisir yang dijelaskan sebagai berikut: [4]

a. Identifikasi Jenis Ransomware
   Pada awalnya telah diidentifikasi bahwa BSI menjadi korban ransomware, dengan jenis ransomware yang disebut Lockbit. Ransomware adalah jenis serangan siber di mana peretas mengenkripsi data korban dan meminta tebusan agar data tersebut dapat dikembalikan.
b. Penemuan Kebocoran Data
   Kelompok ransomware Lockbit tidak hanya mengancam, tetapi juga telah berhasil mencuri dan mengenkripsi data sebesar 1,5 TB milik BSI. Proses pencurian data yang sebesar itu membutuhkan waktu yang sangat panjang, mengindikasikan bahwa peretasan ini merupakan serangan yang terorganisir dan cermat.
c. Tanggal Kejadian
   Kejadian peretasan kemungkinan besar terjadi sebelum tanggal 8 Mei 2023. Pada tanggal tersebut, terjadi error pada aplikasi BSI Mobile yang membuatnya tidak dapat digunakan.
d. Analisis Waktu Pencurian Data
   Pakar keamanan siber memberikan perhitungan terkait waktu pencurian data. Dengan asumsi pencurian dilakukan secara kontinu selama 24 jam dengan kecepatan transfer data 25 Mbps, diperkirakan waktu yang dibutuhkan untuk mencuri dan mengenkripsi data sebesar 1,5 TB adalah 6 hari. Namun, Alfons juga mencatat bahwa peretasan dilakukan dengan hati-hati untuk menghindari kecurigaan, yang dapat memperpanjang waktu pencurian menjadi 12 hari.
e. Dampak Kebocoran Data
   Salah satu dampaknya adalah ekspos kondisi keuangan nasabah yang memiliki saldo tidak wajar. Selain itu, data sensitif seperti kredensial m-banking, internet banking, dan email berpotensi bocor, mengancam keamanan informasi pribadi nasabah dan karyawan.

Di dunia perbankan, penegakan dan perlindungan hukum terhadap nasabah sebagai konsumen sangat penting karena hubungan antara badan usaha dan konsumen sangat penting. Perjanjian yang dibuat oleh nasabah untuk menggunakan layanan perbankan yang didasarkan pada persetujuan kedua belah pihak hanya dapat ditandatangani oleh bank,

[4] Maulana, Nicky, et al. "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah." *Innovative: Journal Of Social Science Research* 4.1 (2024): 8244-8258.

pihak yang memiliki otoritas lebih tinggi. Selama ini, klien hanya dapat menerima atau menolak transaksi yang ditawarkan bank. Adanya peraturan dan kebijaksanaan yang relevan adalah salah satu upaya perlindungan hukum yang penting.[5]

Undang-undang ITE (Informasi dan Transaksi Elektronik) dan Peraturan Otoritas Jasa Keuangan (OJK) tentang keamanan informasi dan transaksi elektronik adalah beberapa undang-undang yang dibuat oleh pemerintah Indonesia untuk mengatur keamanan dan perlindungan data. Untuk melindungi data pelanggan, undang-undang ini menetapkan protokol yang jelas yang harus diikuti oleh Bank Syariah Indonesia. Ini termasuk penggunaan teknologi keamanan yang tepat, prosedur pencegahan peretasan, dan pelaporan insiden keamanan.

Selain undang-undang, perlindungan hukum juga mencakup sanksi bagi mereka yang melakukan peretasan data. Undang-Undang ITE Indonesia memberikan dasar hukum untuk menindak tegas mereka yang melakukan peretasan data. Orang yang terbukti melakukan peretasan data dapat dikenakan hukuman pidana, seperti penjara dan denda. Tujuan dari sanksi ini adalah untuk memberikan efek jera kepada mereka yang melakukan peretasan dan mendorong orang lain untuk tidak melakukan hal yang sama lagi. Selain itu, perlindungan hukum dimaksudkan untuk melindungi klien Bank Syariah Indonesia. Bank bertanggung jawab atas kerahasiaan data pelanggan dan bertanggung jawab atas kerugian yang ditimbulkan akibat peretasan data. Jika terjadi kerugian materil, pelanggan memiliki hak untuk mendapatkan ganti rugi.

Dalam situasi peretasan, pengguna Bank BSI perlu menggunakan kebijakan hukum yang ada sebagai bentuk perlindungan atas data pribadi mereka. Kebijakan kriminalisasi atau rumusan hukum pidana di Indonesia terkait permasalahan cybercrime selama ini dapat diidentifikasi sebagai berikut:[6]

a. Dalam KUHP

Rumusan tindak pidana dalam KUHP sebagian besar masih konvensional dan belum berkaitan langsung dengan perkembangan *cyber crime*. Selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan kejahatan teknologi tinggi yang sangat bervariasi. Misalnya, KUHP kesulitan menangani pemalsuan kartu kredit dan transfer dana elektronik karena tidak ada aturan khusus mengenai hal tersebut. Ketentuan yang ada hanya menyangkut:

1) sumpah/pernyataan palsu (Pasal 242);
2) menghindari mata uang dan uang kertas (Pasal 244-252);
3) pemalsuan stempel dan tanda (Pasal 253-262); dan
4) pemalsuan surat (Pasal 263-276)7.

b. Undang-Undang di luar KUHP

1) Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi mengancam tindak pidana terhadap a) Memanipulasi akses ke jaringan telekomunikasi (Pasal 50 jo. Pasal 22); b) Mengakibatkan gangguan fisik dan elektromagnetik pada penyelenggaraan telekomunikasi (Pasal 55 jo. Pasal 38); c) Melakukan penyadapan atas informasi melalui jaringan telekomunikasi (Pasal 56 jo. Pasal 40);

[5] Keliat, Venia Utami, et al. "Analisis Upaya Dan Peran Perlindungan Hukum Terhadap Kasus Peretasan Data Bank Syariah Indonesia." Ilmu Hukum Prima (IHP) 6.2 (2023): 182-190.
[6] Kasim, Zainuddin. "Kebijakan Hukum Pidana Untuk Penanggulangan *Cyber Crime* Di Indonesia." *Indragiri Law Review* 2.1 (2024): 21-22.

2) Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan atas UU No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi; Pasal 38 UU No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang; dan Pasal 44 ayat (2) UU No. 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi, mengakui rekaman elektronik sebagai alat bukti yang sah;

c. **Undang-Undang Nomor 32 Tahun 2002** tentang Penyiaran, antara lain mengatur tentang tindak pidana: 1) Pasal 57 jo. 36 ayat (5) mengancam pidana terhadap siaran yang: a) bersifat fitnah, menghasut, menyesatkan, atau bohong; b) menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau c) mempertentangkan suku, agama, ras, dan antargolongan; 2) Pasal 57 jo. Pasal 36 ayat (6) mengancam pidana terhadap siaran yang memperolokkan, merendahkan, melecehkan, atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional; 3) Pasal 58 jo. 46 ayat (3) mengancam pidana siaran iklan niaga yang memuat: a) promosi yang berhubungan dengan ajaran suatu agama, ideologi, perseorangan, atau kelompok, yang menyinggung perasaan atau merendahkan martabat orang lain, ideologi lain, perseorangan lain, atau kelompok lain; b) promosi minuman keras atau sejenisnya serta zat atau bahan yang bersifat adiktif; c) promosi rokok yang memperagakan wujud rokok; d) hal-hal yang bertentangan dengan kesusilaan dan nilai-nilai agama; atau e) eksploitasi anak di bawah umur;

d. **UU Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008** tentang Informasi dan Transaksi Elektronik (UU-ITE), memuat ketentuan pidana bagi setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen.

Dalam kasus peretasan data Bank BSI, undang-undang di atas menetapkan kebijakan dan standar etika yang harus dipatuhi oleh pelaku kejahatan kriminal tersebut. Dijelaskan bahwa Pasal 36 PERMEN Komunikasi dan Informatika Nomor 20 Tahun 2016 menetapkan sanksi berupa teguran lisan dan tertulis, penghentian kegiatan, dan pengumuman di situs web. Ketentuan ini berasal dari alinea pertama Pasal 26 UU Nomor 19 Tahun 2016, yang menetapkan bahwa persetujuan individu diperlukan sebelum penggunaan data pribadi secara elektronik.

Berbeda hal dengan peretasan Bank BSI di mana pencurian telah berkembang. Ini disebabkan fakta bahwa peretasan situs web tidak sama dengan pencurian tradisional. Dalam pencurian tradisional, pencuri harus secara aktif menghadapi objek tersebut dan mendekatkan tangan dan jari mereka dengan objek tersebut. Pelakunya terhubung dengan komputer yang terhubung dengan jaringan internet di rumah atau dengan menyewa lokasi yang menawarkan layanan jaringan internet, bukan barangnya sendiri, sehingga pencurian ini berbeda dengan pencurian melalui website. *Joy Computing* juga didefinisikan sebagai tindakan menggunakan komputer secara ilegal, tanpa izin, atau tanpa otoritas, yang disamakan dengan tindak pidana pencurian menurut Pasal 362 KUHP. Selain itu, peretasan pengguna Bank BSI yang berkaitan dengan UU No. 11/2008 tentang Informasi dan Transaksi Elektronik diatur dalam Pasal 30, Pasal 46, dan Pasal 52. Pasal-pasal tersebut menunjukkan bahwa tindakan perlawanan hukum yang disengaja untuk mengakses komputer atau media elektronik dengan cara yang salah dikenai sanksi yang tercantum masing-masing

didalamnya. Oleh karena itu, perlu diketahui bahwa tindakan kriminal yang berkaitan dengan peretasan pengguna Bank BSI tersebut harus ditinjau termasuk dalam jenis tindak kejahatan yang tercantum dalam Pasal-pasal delik ITE tersebut. Hal ini disebabkan fakta bahwa tindakan yang merugikan orang lain dapat disebut sebagai "peretasan". [7]

2. Upaya pencegahan dan penanggulangan kejahatan siber terhadap data pengguna Bank Syariah Indonesia (BSI)

Terdapat beberapa upaya pencegahan dan penanggulangan kejahatan siber terhadap data pengguna Bank Syariah Indonesia (BSI) yang melibatkan berbagai strategi yang dirancang untuk melindungi nasabah dan menjaga integritas sistem perbankan. Berikut adalah langkah-langkah yang diambil oleh BSI dan sektor perbankan secara umum:[8]

1. Penguatan Keamanan Sistem
   a. Tim Keamanan Informasi: BSI telah menganggarkan dana sebesar Rp 580 miliar untuk memperkuat aspek digitalisasi dan keamanan data nasabah. BSI menegaskan bahwa alokasi anggaran tersebut akan difokuskan pada penguatan sistem pengamanan data dan layanan perbankan. BSI memiliki tim khusus yang bertanggung jawab untuk menjaga keamanan data, termasuk penguatan parameter keamanan seperti *firewall* dan *threat intelligence*. Tim ini juga melakukan pengujian keamanan secara berkala untuk mendeteksi potensi ancaman
   b. Penggunaan Teknologi Keamanan: Penerapan teknologi canggih seperti autentikasi multi-faktor dan monitoring keamanan jaringan membantu mencegah akses tidak sah dan serangan siber
2. Edukasi dan Kesadaran Nasabah
   a. Program Edukasi: BSI melaksanakan program edukasi untuk meningkatkan kesadaran nasabah tentang pentingnya keamanan data pribadi. Ini dilakukan melalui berbagai saluran seperti aplikasi mobile, media sosial, dan webinar
   b. Verifikasi Identitas: Nasabah dianjurkan untuk selalu memverifikasi identitas pihak yang meminta informasi sensitif, serta waspada terhadap permintaan yang mencurigakan
3. Kebijakan Privasi dan Transparansi
   a. Kebijakan Privasi yang Jelas: BSI memastikan bahwa kebijakan privasi mereka dipahami oleh nasabah, dengan evaluasi berkala untuk menilai efektivitasnya
   b. Transparansi dalam Penanganan Insiden: Dalam hal terjadi kebocoran data, BSI diwajibkan untuk segera memberi tahu nasabah tentang pelanggaran, termasuk rincian data yang terpengaruh dan langkah-langkah pemulihan yang diambil
4. Kerjasama dengan Pihak Ketiga

   Monitoring Eksternal: BSI bekerja sama dengan pihak ketiga untuk memantau privasi nasabah dan melaporkan hasilnya kepada regulator seperti Kementerian Komunikasi dan Informatika (Kominfo)

[7] 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* 2.1 (2024): 244.

[8] Diny Luthfah, "Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia", Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti, 9 (2023), 259

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 9 No 11 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

KESIMPULAN

Penelitian ini memberikan pemahaman terhadap penegakan hukum dalam menanggulangi kejahatan siber dan pengelolaan keamanan yang dapat diterapkan oleh Bank Syariah Indonesia (BSI). Dengan pertumbuhan ekonomi digital yang pesat, menjaga keamanan nasabah saat menggunakan layanan perbankan digital menjadi sangat penting. Pelaksanaan kebijakan keamanan dan penegakan hukum yang kuat akan menjadi kunci keberlanjutan dan kepercayaan nasabah di era ekonomi digital.

Saran yang dapat dipertimbangkan yaitu periksa undang-undang dan peraturan nasional yang mengatur perbankan dan perlindungan data. Kemudian memeriksa perjanjian dan kebijakan bank untuk melihat peraturan tentang keamanan data dan bagaimana bank bertanggung jawab untuk melindungi data pelanggan. Pastikan bahwa bank telah memenuhi kewajibannya sesuai dengan perjanjian. Laporkan kebocoran data pelanggan kepada bank dan pihak berwenang yang relevan, seperti otoritas pengawas perbankan atau lembaga yang bertanggung jawab atas perlindungan data pribadi. Konsultasikan dengan ahli hukum yang berpengalaman dapat membantu mengevaluasi situasi yang sedang terjadi, memberikan nasihat hukum yang tepat, dan membantu dan melindungi hak-hak sebagai nasabah.

Peninjauan prosedur dengan memeriksa ketentuan dalam perjanjian yang berkaitan dengan penyelesaian sengketa antara pelanggan dan bank untuk menilai proses penyelesaian sengketa. Jika data pelanggan bocor, maka dapat menuntut ganti rugi. Dalam hal ini, konsultasikan dengan ahli hukum untuk memahami proses hukum yang terkait dengan klaim ganti rugi dan mengumpulkan bukti yang kuat tentang kerugian yang dialami.

DAFTAR PUSTAKA

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diubah dengan UU No. 19 Tahun 2016

Ratulangi, C. H. (2021). Tindak pidana cyber crime dalam kegiatan perbankan. *Lex Privatum*, *9*(5).

Maulana, N., Laurens, T., Faiz, D. H. A., & Patrianti, T. (2024). Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah. *Innovative: Journal Of Social Science Research*, *4*(1), 8244-8258.

Keliat, V. U., Siregar, A. P., Zulkifli, S., & Purba, I. (2023). Analisis Upaya dan Peran Perlindungan Hukum Terhadap Kasus Peretasan Data Bank Syariah Indonesia. *Ilmu Hukum Prima (IHP)*, *6*(2), 182-190.

Kasim, Z. (2024). Kebijakan Hukum Pidana Untuk Penanggulangan Cyber Crime Di Indonesia. *Indragiri Law Review*, *2*(1), 18-24.

Tirta, G. A., & Lie, G. (2024). Tinjauan Hukum Terhadap Tindak Pidana *Cyber crime* dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI). *MANTAP: Journal of Management Accounting, Tax and Production*, *2*(1), 240-249.

Luthfah, D. (2024). Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia. *Jurnal Penelitian dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, 259-267.