MANTAP: Journal of Management Accounting, Tax and Production
E-ISSN: 3025-7786 P-ISSN: 3025-7794
Vol. 2 No. 1 Maret 2024

Tinjauan Hukum Terhadap Tindak Pidana Cybercrime dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI)

George Anderson Tirta[1] Gunardi[2]
Universitas Tarumanagara, Kota Jakarta Barat, Provinsi DKI Jakarta, Indonesia[1,2]
Email: george.205220252@stu.untar.ac.id[1]

Abstrak

Bank merupakan komponen penting dalam sistem keuangan suatu negara, dan integritasnya adalah kunci bagi kelangsungan perekonomian dan keuangan masyarakat. Ancaman seperti peretasan data dan kejahatan dunia maya lainnya semakin meresahkan bank, dengan contoh nyata seperti kasus Bank BSI yang mengalami peretasan data pada tahun 2023. Pada penelitian ini akan membahas dua identifikasi masalah yakni Pertama, aspek hukum yang terkait dengan tindak pidana cybercrime, khususnya peretasan data pengguna Bank BSI dan Kedua, upaya pencegahan yang dapat dilakukan untuk melindungi data penggunaan Bank BSI dari tindak pidana cybercrime, terutama peretasan data. Jenis penelitian yang digunakan adalah yuridis normatif dengan pendekatan peraturan-undangan maupun pendekatan konteks. Dalam konteks tindak pidana peretasan data pengguna Bank BSI, terdapat beberapa aspek hukum yang relevan yang harus diperhatikan. Aspek-aspek hukum ini mencakup: Pasal 362 KUHP, PP No 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika No 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, UU No. 24 Tahun 2013 Administrasi Tentang Kependudukan dan UU No 14 Tahun 2008 Tentang Keterbukaan Informasi Publik. Untuk melindungi data pengguna Bank BSI dari peretasan data, langkah-langkah yang kuat dalam pemantauan dan perlindungan keamanan data sangatlah penting. Hal ini meliputi penguatan sistem keamanan internal bank, pelatihan cybersecurity bagi karyawan, pemantauan rutin terhadap potensi ancaman, serta kerja sama yang erat dengan pihak eksternal.

Kata Kunci: Hukum, Cybercrime, Bank BSI

PENDAHULUAN

Pesatnya pertumbuhan teknologi data dan surat menyurat secara keseluruhan berdampak pada banyak aspek kehidupan, termasuk sektor keuangan. Keamanan data nasabah bank terancam serius dengan adanya peretasan informasi. Bahkan di era globalisasi saat ini, bank telah mengintegrasikan diri ke dalam sistem pembayaran dan keuangan global. Bank adalah komponen dari sistem keuangan sistem pembayaran suatu negara. Berdasarkan faktor-faktor tersebut, suatu bank menjadi milik umum apabila mendapat izin dari otoritas moneter negara untuk hidup dan berfungsi. Akibatnya, masyarakat luas dan di rumah, selain pemilik bank, harus memastikan kelangsungan hidupnya. Sebagai bagian dari sistem pembayaran suatu negara, bank tidak dapat dipisahkan dari aktivitas kriminal. Kurangnya kesadaran akan bahaya yang mereka hadapi telah menyebabkan kematian banyak korban. Skimming dan rekayasa sosial adalah dua jenis kejahatan paling umum yang dilakukan di industri jasa keuangan. Skimming adalah bentuk umum pencurian informasi yang melibatkan penyalinan informasi dari strip magnetik kartu kredit atau debit tanpa izin.

Salah satu kasus bank yang mengalamai aktivitas kriminal yakni Bank BSI. Bank BSI sebagai yayasan keuangan yang menggunakan layanan online juga menghadapi pertaruhan serupa. Peretasan data dan bentuk kejahatan dunia maya lainnya telah muncul sebagai masalah hukum utama. Selanjutnya, yayasan ini akan mengkaji perspektif legitimasi yang terkait dengan pelanggaran cybercrime, khususnya peretasan informasi nasabah Bank BSI, serta sebagai

perkiraan preventif yang dapat diambil untuk melindungi informasi nasabah Bank BSI dari kejahatan cybercrime. Penelitian peretasan dan dugaan pencurian data di Bank Syariah Indonesia (BSI) sedang dilakukan oleh Badan Reserse Kriminal (Bareskrim) Direktorat Tindak Pidana Siber (Dittipidisiber) Polri. Hal ini diinformasikan melalui kutipan kronologi yang diterbitkan di halaman resmi Kompas.com. Tim peretas yang menggunakan program komputer bernama LockBit berhasil menguasai sistem komputer Badan Standarisasi Nasional (BSI). Sebelum mengalami peretasan pada tanggal 8 Mei 2023, sistem BSI juga mengalami kerusakan yang mengakibatkan crash. Informasi yang dapat mencakup alamat, nomor telepon, jumlah uang yang tersimpan di rekening, catatan transaksi, tanggal pembukaan rekening, data pekerjaan, dan informasi lainnya, termasuk data yang terungkap. Data yang terbocor tentang klien mencakup identitas pribadi seperti nama, nomor telepon, alamat, perubahan akun, sejarah transaksi, tanggal pembuatan akun, informasi pekerjaan, dan berbagai detail lainnya.

Pelanggaran kejahatan dunia maya menggabungkan berbagai operasi kriminal yang dilakukan melalui organisasi kompter dan internet. Salah satu jenis cybercrime yang sering terjadi adalah information hacking. Dalam konteks Bank BSI, akan dijelaskan secara rinci pengertian peretasan data dan komponen-komponennya. Kewajiban hukum dalam kejahatan dunia maya mencakup perspektif yang berbeda, seperti lokal, bukti elektronik, dan pelaksanaan persetujuan. Pihak-pihak yang terkait dengan peretasan informasi, baik sebagai penghibur dasar maupun penghibur yang mengambil bagian, dapat bergantung pada otorisasi yang sah sesuai pedoman materi. Korban peretasan data, termasuk pengguna Bank BSI yang menjadi target penyerangan dilindungi undang-undang. Memulihkan akses akun, memberikan kompensasi kepada korban, dan merehabilitasi mereka hanyalah beberapa tindakan hukum yang harus diambil untuk memastikan bahwa kerugian dapat diperoleh kembali dan konsekuensi dari pelanggaran data dikurangi. Pelaku cybercrime seringkali berasal dari berbagai negara. Oleh karena itu, kolaborasi di seluruh dunia dalam menaklukkan kejahatan dunia maya sangatlah penting.

Ketentuan hukum pidana di Indonesia, termasuk yang tercantum di dalam KUHP dan peraturan perundang-undangan selain KUHP, contohnya Undang-Undang Nomor n Pada tahun 2008, disahkan UU No. 11 Teks ini membahas mengenai UU No. 19 Tahun 2016 mengenai Transaksi dan Informasi Elektronik. Namun, keunikan tentang kualitas kejahatan online dan sistem hukum pidana di Indonesia tidak bisa diabaikan. Perkembangan KUHP, contohnya, menganggap istilah "terbuka" serupa dengan "daring" dan "mengakses halaman yang dibatasi" seperti yang dijelaskan dalam KUHP untuk mencoba situasi "memasuki ruang angkasa" sangat rumit untuk dilakukan. digunakan sebagai alasan untuk melakukan kejahatan dalam dunia digital. Di internet, para pengguna tidak diperbolehkan mengakses informasi yang dimiliki oleh individu lain (akses ilegal). Mengingat Pasal 4 UU No 19/2016 tentang Informasi dan Transaksi Elektronik menjelaskan bagaimana transaksi elektronik dan teknologi informasi digunakan untuk:

1. menginformasikan partisipasi bangsa dalam masyarakat informasi global;
2. menumbuhkan perekonomian dan perdagangan bangsa dengan tujuan mensejahterakan kehidupan masyarakat;
3. bekerja pada kecukupan dan efektivitas administrasi publik;
4. membuka kesempatan yang seluas-luasnya bagi setiap orang untuk mengembangkan daya pikir dan kemampuannya dalam bidang pemanfaatan dan pemanfaatan inovasi informasi seideal mungkin yang diharapkan dan benar untuk dibentuk dan diketahui;
5. memberikan pengguna dan penyedia layanan TI rasa aman, keadilan, dan kepastian hukum.

Sebagaimana disebutkan dalam tujuan diatas dalam Pasal 4, penggunaan inovasi data dan pertukaran elektronik oleh inovator saat ini tidak sejalan dengan apa yang diharapkan secara

umum dari Peraturan Informasi dan Transaksi Elektronik. Kehidupan individu telah dipengaruhi oleh kejahatan dunia maya di mana-mana. Teknologi informasi saat ini menjadi pedang bermata dua karena juga merupakan alat yang ampuh untuk melanggar hukum dan meningkatkan kesejahteraan, kemajuan, dan peradaban manusia. Rumusan Masalah: Mengingat klarifikasi permasalahan di atas, berikut ini permasalahan yang menyertai dikumpulkan oleh penulis: Bagaimana aspek hukum yang terkait dengan tindak pidana cybercrime, khususnya peretasan data pengguna Bank BSI? Bagaimana upaya pencegahan yang dapat dilakukan untuk melindungi data penggunaan Bank BSI dari tindak pidana cybercrime, terutama peretasan data?

METODE PENELITIAN

Tipe penelitian ini menggunakan penelitian normatif yang bersifat teoritis serta menafsirkan dan menerapkan aturan-aturan yang berkaitan dengan asas, konsep, doktrin dan norma yang berlaku dalam hukum positif. Penelitian ini berdasarkan normatif dikenal sebagai penelitian hukum doktrinal yang memberikan penjelasan secara sistematis tentang norma untuk aspek tertentu, menganalisis hubungan antara norma hukum satu sama lain, dengan memperhatikan penelitian analisis pada hukum dan peraturan. Penelitian ini menggunakan Pendekatan Perundang-Undangan (Statute Approach) dan Pendekatan Konseptual . Tujuan penelitian ini untuk memberikan perspektif sebagaimana memecahkan dan menemukan jawaban dari isu hukum . Penelitian dalam bidang hukum terdapat dua macam yakni bahan hukum primer dan bahan hukum sekunder. Teknik Pengumpulan Bahan Hukum dengan cara perolehan bahan hukum dilakukan dengan ilmu keperpustakaan (dokumen) yang mana ilmu ini berkaitan dengan pendalaman bahan hukum tertulis. Penulis mengidentifikasi bahan-bahan hukum yang diperoleh kemudian memahami dan mencatat keselarasan dengan penelitian yang dilakukan. Proses penelitian data yang telah dikumpulkan dan diolah dikenal dengan pengelolaan data. Biasanya, pemeriksaan data, evaluasi, rekonstruksi data, dan sistemisasi data. Penulis penelitian ini menggunakan analisis data dan pengecekan data (editing). Penulis menggunakan analisis deduktif dalam analisis bahan hukum .

HASIL PENELITIAN DAN PEMBAHASAN

Aspek Hukum yang Terkait Dengan Tindak Pidana Cybercrime, Khususnya Peretasan Data Pengguna Bank BSI

Bank BSI merupakan salah satu contoh bank yang menjadi sasaran tindak kriminal. Sebagai lembaga keuangan berbasis online, Bank BSI menghadapi risiko serupa. Kejahatan dunia maya, termasuk peretasan data, telah muncul sebagai masalah hukum utama pada penelitian ini. Selain itu, yayasan ini akan menyelidiki keabsahan kejahatan dunia maya, khususnya peretasan data nasabah Bank BSI, serta langkah-langkah yang dapat diambil untuk melindungi data nasabah Bank BSI dari kejahatan dunia maya. Dari cerita yang tertera di situs Kompas.com, terlihat dengan jelas bahwa Bareskrim Dittipidisiber Polri telah memulai penyelidikan terhadap kasus peretasan dan diduga pencurian data di BSI. LockBit, sebuah kelompok pengembang perangkat lunak, berhasil masuk ke sistem BSI. Sebelum mengalami serangan hack pada tanggal 8 Mei 2023, sistem BSI juga mengalami kegagalan. Data yang disimpan dalam sistem termasuk alamat, jumlah uang di rekening, catatan transaksi, tanggal dibukanya rekening, informasi pekerjaan, dan berbagai data lainnya, termasuk informasi yang telah dibocorkan. Data klien yang tumpah mencakup nama, nomor telepon, alamat, perubahan akun, riwayat perdagangan, tanggal pembukaan akun, informasi pekerjaan, dan data lainnya. Untuk melakukan tindakannya, peretas harus memiliki keterampilan komputer dasar, termasuk:

1. Sedikit dapat mempelajari bahasa pemrograman komputer.
2. Mampu mencari, mempelajari, dan mengoperasikan salah satu versi Unix sumber terbuka.
3. Kemampuan untuk menulis hypertext markup language (HTML) untuk memahami sistem situs web dan mempelajarinya.

Memasukkan arah yang tidak valid, misalnya seseorang secara ilegal memasukkan petunjuk untuk membuat kerangka kerja PC memindahkan aset dimulai dengan satu catatan lalu ke catatan berikutnya. Hal ini dapat dilakukan oleh pegawai bank atau pihak luar yang berusaha mendapatkan akses ke sistem komputer tanpa izin. Informasi input diubah, misalnya informasi yang secara sah masuk ke PC sengaja diubah. Metode ini paling sering digunakan karena mudah diterapkan tetapi sulit dilacak kecuali diperiksa secara teratur. Salah satu bentuk perilaku menyimpang tersebut adalah kejahatan atau perilaku kriminal. Menurut Prof. Sudarso, pertimbangan-pertimbangan berikut ini harus diperhatikan dalam menangani tindak pidana atau masalah yang berkaitan dengan tindak pidana:

1. Menggunakan hukum pidana untuk kepentingan pembangunan nasional harus memperhatikan terciptanya masyarakat yang adil, makmur, dan merata secara spiritual dan material berdasarkan Pancasila. Berkaitan dengan hal tersebut, pemanfaatan pengaturan pidana diarahkan untuk menangani kesalahan dan menahan imbalan atas penanggulangan yang sebenarnya, untuk bantuan pemerintah dan jaminan masyarakat.
2. Pelanggaran yang menimbulkan kerugian fisik atau spiritual pada anggota masyarakat harus memenuhi syarat sebagai "tindakan yang tidak diinginkan" agar dapat dihukum secara pidana.
3. Penggunaan hukum pidana juga harus memperhatikan konsep “biaya dan hasil”.
4. Kapasitas kerja atau kemampuan aparat penegak hukum juga harus diperhatikan, sehingga tidak boleh terjadi overloading.

Sementara menurut Prof. Dr. Wirjono Prodjikoro, SH berpendapat bahwa tujuan hukum pidana adalah untuk mencapai rasa keadilan. Tujuan hukum pidana, menurut para sarjana hukum, lanjutnya, adalah:

1. Untuk mengejutkan banyak orang (pencegahan umum), serta memperingatkan individu tertentu yang telah melakukan kesalahan sekali lagi (pencegahan luar biasa), atau
2. Membina atau mengembangkan lebih lanjut individu-individu yang telah menunjukkan bahwa mereka suka melakukan kesalahan, sehingga mereka menjadi pribadi yang baik, sehingga mereka berguna bagi masyarakat.

Sudut pandang ini hanya dapat diterima sebagai tujuan sekunder atau tambahan, dan meskipun bersifat tambahan, tujuan ini dapat memainkan peran penting dalam memperbaiki neraca masyarakat, yang merupakan tujuan utama dari sanksi pidana, sanksi administrasi, dan sanksi perdata. Menurut pendapat dari Berda Nawawi Arief, melihat bahwa ungkapan “Kebijakan” diambil dari ungkapan “police” (Inggris) dan “politiek” (Belanda), sehingga “Politik Hukum Pidana” dapat disinggung juga sebagai “Permasalahan Peraturan Perundang-undangan Pidana” dan yang sering dikenal dengan istilah “reformatory approach”, “criminal regulation arrangement” atau “strafrechpolitiek”. Dalam situasi peretasan, pengguna Bank BSI perlu menggunakan kebijakan hukum yang ada sebagai bentuk perlindungan atas data pribadi mereka. Jebakan hukum yang dapat digunakan sebagai proses hukum dalam pelaksanaan hukum adalah:

1. Buku peraturan hukum pidana (KUHP)
2. Undang-undang nomor 71 tahun 2019 yang mengatur mengenai pengoperasian sistem dan transaksi elektronik;

3. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 yang Berkaitan dengan Pengamanan Informasi Pribadi dalam Sistem Elektronik.
4. UU No 24/2013 yang berjudul Perubahan terhadap Undang-Undang Nomor 23 Tahun 2006 mengenai Administrasi Kependudukan, merupakan aturan hukum yang mengubah ketentuan dalam Undang-Undang tersebut.
5. UUD No 19/2016 yang berjudul Informasi serta Transaksi Digital merupakan sebuah perundangan yang mengatur mengenai kegiatan serta peraturan terkait penggunaan serta pelaksanaan transaksi elektronik.
6. UU No 14/2008 mengatur mengenai akses publik terhadap informasi di Indonesia.

Adanya undang-undang hukum diatas sebagai aspek hukum bagi kasus peretasan data Bank BSI. Sebagaimana undang-undang menjadi kebijakan dan pedoman aturan kehidupan yang menyimpang agar dikenai sanksi bagi pelaku kejahatan kriminal tersebut. Ditegaskan, Pasal 36 PERMEN Komunikasi dan Informatika Nomor 20 Tahun 2016 dikenakan sanksi berupa teguran lisan dan tertulis, penghentian kegiatan, dan pengumuman di situs online, sebagaimana tertuang dalam. Aturan ini bersumber dari alinea pertama Pasal 26 UU No. 19 Tahun 2016, yang mengatur bahwa persetujuan seseorang harus diperoleh sebelum informasi mengenai data pribadinya dapat digunakan secara elektronik. Kemudian peretasan pada kasus Bank BSI meurpakan tindakan pencuian yang terkandung dalam Pasal 362 KUHP terdapat unsur-unsurnya diantaranya unsur obyektif dan unsur subjektif. Demonstrasi mengambil situasi ini telah maju sesuai dengan sudut pandang sifat kegiatan. Adami mendefinisikan mengambil sebagai perilaku atau aktivitas material konstruktif yang biasanya melibatkan penggunaan otot jari dan tangan yang dikembangkan secara sadar dan secara bersamaan mengoordinasikan jari untuk menyentuh, memegang, dan mengangkat suatu objek tanpa berhenti. itu, kemudian, pada saat itu, menyampaikannya. itu dan gunakan kekuatannya di sana atau pindahkan ke tempat lain.

Akan tetapi dengan kondisi pernyataan tersebut, berbeda hal dengan kasus peretasan Bank BSI yang mana pencurian telah mengalami perkembangannya. Ini karena 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 merupakan tindakan menggunakan komputer secara ilegal, tanpa izin, atau tanpa otoritas, disamakan dengan tindak pidana pencurian menurut Pasal 362 KUHP. Dipertegas pula adanya tindakan peretasan pengguna Bank BSI dikaitan dengan UU No. 11/2008 tentang Informasi dan Transaksi Elektronik, Joy Computing diatur dalam Pasal 30, Pasal 46, dan Pasal 52. Pasal-pasal tersebut menyebutkan bahwa adanya kesengajaan perlawanan hukum atas mengaksesnya kompter atau media elektronik dengan cara yang salah dikenai sanksi yang tercantum masing-masing diidalamnya.

Terdapat 19 jenis tindak pidana dalam Pasal 27 sampai dengan 37 UU Informasi dan Transaksi Elektronik. Di antara 19 jenis pelanggaran ITE, seperti halnya perampokan bank melalui ATM, muncul di dekat perampokan uang tunai melalui buku besar menggunakan kantor web. Tindakan pencuri yang tidak diketahui identitasnya dapat dikualifikasikan (disamakan) dengan tindakan "membobol" sistem keamanan untuk mendapatkan akses ke properti. Melakukan aktivitas semacam itu menjadikan orang lain menderita kerugian. Orang lain yang mengalami kerugian adalah elemen penting yang harus dimasukkan dalam delik ITE yang direncanakan menurut Pasal 30 Ayat (3). Termasuk dalam kategori kerugian ini adalah

Pasal 36. Jika ada kerugian pada orang lain yang terbukti, maka semua jenis pelanggaran yang diatur dalam Pasal 27 hingga 34 dapat dianggap sebagai pelanggaran hukum di bidang Teknologi Informasi dan Elektronika (ITE). Dengan demikian perlu diketahui bahwa tindakan kriminal peretasan pengguna Bank BSI tersebut perlu ditinjau termasuk dalam perbuatan tindak kejahatan yang mana dalam Pasal-pasal delik ITE tersebut dikarenakan dapat disebut "peretasan" apabila suatu tindakan itu telah merugikan orang lain.

Upaya Pencegahan yang Dapat Dilakukan Untuk Melindungi Data Penggunaan Bank BSI Dari Tindak Pidana Cybercrime, Terutama Peretasan Data

Terdapat beberapa langkah preventif yang dapat dilakukan untuk melindungi data penggunaan Bank BSI dari kejahatan dunia maya, khususnya peretasan data. Berikutnya beberapa hal yang perlu diperhatikan sebagai berikut:

1. Aspek Internal Bank BSI
   a. Sistem Keamanan yang Diperkuat Bank BSI harus merangkul dan mengeksekusi kekuatan utama untuk kerangka kerja, misalnya, inovasi enkripsi informasi dan firewall yang diperbarui secara konsisten. Data pengguna dapat dilindungi dan risiko peretasan data berkurang karenanya. Sesuai Peraturan No. 19 Tahun 2016 tentang UU ITE di Indonesia, lembaga keuangan, termasuk bank, diharapkan untuk menjaga informasi milik klien dan mengamankannya dari akses yang tidak sah.
   b. Pelatihan Karyawan. Pelatihan cybersecurity secara berkala wajib diberikan kepada karyawan oleh Bank BSI. Ini akan membantu Bank BSI mengidentifikasi strategi serangan peretas yang khas dan meningkatkan kesadaran akan ancaman keamanan saat ini. Selain itu, Bank BSI harus menerapkan kebijakan keamanan yang ketat, seperti perubahan password yang sering dan penggunaan password yang kuat. Berdasarkan Peraturan BI No. 18/40/PBI/2016 tentang Sistem Keamanan Informasi di Bank, bank diharapkan untuk mengarahkan persiapan biasa bagi pekerja sehubungan dengan administrasi keamanan data.
   c. Pemantauan Keamanan Rutin dan Aktif Bank BSI harus melengkapi pemantauan keamanan dinamis dengan menggunakan kerangka identifikasi gangguan dan perangkat pengecekan organisasi. Ini akan membantu dalam mengidentifikasi serangan yang sedang berlangsung atau potensi ancaman sistem. Sesuai dengan Pedoman Otoritas Administrasi Moneter (POJK) No. 13/POJK.03/2018 tentang Penyelenggaraan Penatausahaan Pinjaman dan Penerimaan Berbasis Inovasi Data, bank yang menyelenggarakan internet banking diharapkan memiliki komponen untuk membedakan dan menangani kejadian keamanan.
2. Aspek Eksternal
   a. Kualitas Penyelidikan. Agar dapat mengungkap kasus-kasus cybercrime yang dilaporkan oleh masyarakat, penting untuk memperhatikan kapasitas dan kualitas investigasi, serta jumlah pemeriksa yang memadai di setiap unit cybercrime. Peran penting penyidik Polri dalam mengatasi kejahatan online tidak bisa diabaikan. Keberadaan kejahatan komputer dalam lingkungan kepolisian menunjukkan bahwa diperlukan individu yang memiliki keahlian luar biasa di bidang perdagangan informasi dan perangkat keras untuk menangani pelanggaran di dunia maya.
   b. Alat Bukti. Data atau sistem elektronik yang terhubung dengan internet menjadi sasaran atau media kejahatan dunia maya. Selain itu, masih banyak fasilitas umum dan warnet yang gratis. Dari segi pembuktian, cybercrime berbeda dengan kejahatan umum. yang merupakan masalah/penghalang bagi spesialis kejahatan digital.
      1) Bukti Terkomputerisasi Mudah Hilang Jika Tidak Ditangani Secepat Mungkin. Pembuktian dalam kejahatan digital sesuai praktek dalam struktur lanjutan karena

yang dimaksud dalam kejahatan digital adalah informasi atau kerangka elektronik, misalnya dalam hal peretasan, dll atau berpotensi melakukan fitnah atau misrepresentasi Pembuktian dalam kejahatan digital menjadi lebih sulit dibandingkan dengan pembuktian dalam kejahatan konvensional karena semua alat yang digunakan dalam kejahatan digital adalah elektronik dan terkait dengan web. Alat-alat ini mudah diubah, dihapus, atau disimpan oleh pelaku kejahatan digital. Oleh karena itu, secara praktis, pembuktian dalam kejahatan digital menjadi lebih sulit daripada pembuktian dalam kejahatan umum. Secara umum, bukti untuk pelanggaran umum dapat ditemukan dalam struktur aktual yang tidak sulit dihapus, berbeda dengan pelanggaran digital di mana bukti luar biasa dapat dengan mudah dihapus.

2) Penjahat dunia maya melakukan kejahatannya dengan menggunakan fasilitas publik. Diketahui bahwa warung internet (warnet) di Indonesia masih beroperasi secara bebas tanpa ada pengaturan atau pengawasan dari pemerintah maupun penegak hukum yang ada sedangkan penyidik dalam melakukan penyidikan kejahatan dunia maya adalah melacak pelaku berdasarkan alamat server atau informasi alamat IP dari elektronik pelaku. perangkat. Dalam hal ini tentunya menjadi kendala dalam penangkapan pelaku dan pembuktian akan semakin rumit. Banyak pelaku kejahatan dunia maya menggunakan fasilitas publik untuk mengakses dan melakukan sesuatu dengan media elektronik dengan koneksi internet. Hal ini juga dimanfaatkan oleh para penjahat dunia maya sehingga jejak digital mereka tidak bisa dijadikan bukti atau sulit dibuktikan.
3) Saksi berada di tempat yang berbeda dengan pelaku dan korban. Meskipun keterangan saksi sangat penting dalam upaya menegakkan hukum, terutama dalam kasus kejahatan dunia maya. Menurut Pasal 184 ayat (1) huruf a KUHAP, keterangan saksi dianggap sebagai alat bukti yang sah. Namun, dalam kasus kejahatan dunia maya, pembuktian yang melibatkan saksi memiliki perbedaan signifikan dengan kejahatan umum. Dalam kejahatan cyber, saksi tidak perlu berada di tempat yang sama dengan korban maupun pelaku. Ahli yang memantau korban dalam kasus kejahatan digital memiliki peran yang sangat penting dan jarang ada pengamat dalam kasus kejahatan digital karena saksi korban sering kali berada di luar daerah atau bahkan di luar negeri. Hal ini mengakibatkan kesulitan bagi para ahli untuk memeriksa saksi. dan mencatat akibat dari pemeriksaan tersebut. Silahkan rekan menggambarkan ulang teks yang dimaksudkan. Tambahan lagi, Jaksa Penuntut Umum menolak menerima dokumen kasus yang tidak menyertakan laporan resmi dari saksi, terutama saksi korban. Hal ini dikarenakan kemungkinan besar saksi tersebut tidak bisa hadir di pengadilan karena jarak antara tempat tinggal mereka dan pengadilan yang cukup jauh. Jarak yang jauh menyebabkan kekurangan bukti. Apabila berkas kasus diajukan ke pengadilan untuk diproses, ada kemungkinan terdakwa tidak akan dianggap bersalah.

c. Fasilitas. Dalam situasi kejahatan online yang membutuhkan dukungan teknis bagi kepolisian dan penyidik, laboratorium forensik komputer digunakan untuk mengidentifikasi informasi digital dan menyimpan bukti dalam bentuk file digital. Dalam program ini, dapat ditemukan berbagai elemen seperti suara, gambar, kode HTML, dan lainnya. Forensik komputer, yang juga dikenal sebagai forensik digital, bertujuan untuk memastikan keamanan sistem informasi dengan cara mengumpulkan, menganalisis, dan mengamankan berbagai data objektif terkait insiden atau pelanggaran keamanan. Ini akan menjadi bukti dalam persidangan.
d. Yuridiksi. Kejahatan siber adalah tindakan kejahatan yang dilakukan di lintas batas negara karena pelaku dan korbannya dapat berasal dari berbagai negara yang berbeda

dan tidak memiliki kewarganegaraan yang sama. Maka, terdapat keterbatasan mengenai aspek berlokasi saat mengatur tindak kejahatan di dunia maya. Pada umumnya, peraturan hukum pidana berlaku di dalam batas negara (standar regional) dan hanya berlaku untuk warga negara (aturan individu dan publik yang berubah-ubah), serta hanya beberapa pelanggaran tertentu yang bisa diterapkan pada panduan publik yang melibatkan banyak orang, termasuk kejahatan di dunia maya.

1) Orang yang menjadi korban kejahatan dunia maya tetapi tidak mematuhi hukum yang sama dengan Indonesia. Dalam hal yurisdiksi, menghadapi tantangan untuk mengatasi kejahatan maya yang melintasi batas-batas negara menjadi lebih sulit, terutama ketika penjahat maya berasal dari negara di mana peraturan dan aturan yang sama seperti di Indonesia tidak ditegakkan atau diikuti. Dalam konteks lokal, secara spesifik disebutkan dalam Pasal 2 Undang-Undang Nomor 19 Tahun 2016, terutama dalam situasi yang memiliki konsekuensi negatif terhadap kepentingan Indonesia dan dampaknya berpengaruh pada wilayah hukum Indonesia atau di luar yurisdiksi Indonesia.
2) Warga Digital Wrongdoing Pihak yang bersalah yang tidak memiliki hubungan damai dengan Indonesia. Mengenai perspektif yurisdiksi, terutama dalam kasus ini, menghadapi kejahatan dunia maya transnasional akan sulit karena setiap negara memiliki peraturan yang berbeda untuk mengatur dan melindungi penduduk dan negaranya. Untuk kasus peretasan di mana korban adalah penduduk Indonesia atau warga negara Indonesia, namun pelakunya adalah penduduk dari negara yang tidak memiliki hubungan baik dengan Indonesia, pihak penegak hukum akan menghadapi tantangan dalam menangani situasi ini. Hal ini akan menjadi kendala bagi pelaku kejahatan digital dalam menjalani proses hukum, terutama bagi negara-negara yang tidak memiliki hubungan strategis dengan Indonesia seperti Israel, Makau, Korea Utara, Georgia, dan negara-negara lainnya.

KESIMPULAN

Dalam konteks tindak pidana peretasan data pengguna Bank BSI, terdapat beberapa aspek hukum yang relevan. Berikut adalah mengenai aspek hukum yang terkait dengan kejahatan dunia maya, antara lain yakni Pertama, Pasal 362 KUHP: Unsur pencurian seperti mengambil dan memiliki barang secara melawan hukum dapat diterapkan dalam rangka peretasan data. Selanjutnya, PP Nomor 71 Tahun 2019 tentang Pelaksanaan Sistem dan Transaksi Elektronik menyatakan bahwa Bank BSI harus mematuhi aturan ini serta menjaga perlindungan data pengguna dari ancaman cybercrime. Bank BSI harus memastikan keamanan data pengguna dan mematuhi peraturan perlindungan data pribadi yang diberlakukan oleh Menteri Komunikasi dan Informatika melalui No 20 Tahun 2016. Untuk keempat kalinya, Undang-Undang Nomor n menjadi perhatian utama. Pada tahun 2013, diterbitkan peraturan mengenai Administrasi Kependudukan yang menjadi pedoman dalam menjaga kerahasiaan informasi personal nasabah Bank BSI terkait dengan administrasi kependudukan. Akhirnya, undang-undang nomor 14 tahun 2008 mengenai pengungkapan informasi publik.: Dalam konteks peretasan data, akses informasi publik secara ilegal melalui peretasan dapat melanggar undangundang ini. Selanjutnya, untuk melindungi data penggunaan Bank BSI dari peretasan data, Bank BSI perlu memperkuat sistem keamanan internal, memberikan pelatihan cybersecurity kepada karyawan, melakukan pemantauan keamanan rutin, dan bekerja sama dengan pihak eksternal seperti polisi dan laboratorium forensik komputer. Selain itu, kendala yurisdiksi dan perbedaan dalam pembuktian juga perlu diatasi untuk penanganan kejahatan dunia maya yang melibatkan pelaku dan korban dari berbagai negara.

Berdasarkan pemaparan diatas, Penulis memberikan saran bahwa seyogyanya pada pihak Bank BSI untuk memperkuat sistem keamanan internal, memberikan pelatihan cybersecurity kepada karyawan, melakukan pemantauan dan kerjasama yang solid agar tidak terjadi kembali peretasan bagi pengguna Bank BSI. Selanjutnya, seyogyanya kepada pihak masyarakat bahwa tetap mewaspadai tautan yang mencuigakan, menggunakan kata sandi yang kuat dan berbeda untuk setiap akun, dan selalu perbarui perangkat lunak dan system keamanan dengan versi terbaru. Serta terakhir saran Penulis tertuju kepada pihak pemerintah untuk meningkatkan hukuman dan penegakan hukum maupun Pemerintah perlu meningkatkan hukuman bagi pelaku kejahatan dunia maya, termasuk peretasan data bank. Selain itu, penegakan hukum yang efektif dan cepat harus dilakukan untuk memberikan efek jera kepada pelaku kejahatan. Kemudian meningkatkan kerja sama internasional. Lalu, Pemerintah perlu meningkatkan kerja sama dengan negara-negara lain dalam penanggulangan kejahatan dunia maya

DAFTAR PUSTAKA

A.Mahmood et al,. (2020). Intrusion detection system for banking security using an improved random forest algorithm. Computers, Materials & Continua, 63 (1),.

Arief, B.N. (2007). Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia. Raja Grifindo Persada, Jakarta.

Arief, B.N. (2008). Bunga Rampai Kebijakan Hukum Pidana Perkembangan Konsep Baru, Cetakan ke-1. Kencana Prenadamedia Grup, Jakarta

E. Ershov, A. Shorov, and A. Nazarov, (2018). "Data security enhancement method in banking information systems," International Journal of Open Information

Hamamah, F., Apriyani, Y. (2021). Pencurian Uang Pada Rekening Bang Dengan Media Internet (Analisis Kasus Pasal 362 KUHP Jo Undang-Undang RI Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik), FOCUS: Jurnal Of Law, 2 (1)

Hartanto, B.B., & Yulianto, H. (2022). Penegakan Hukum Terhadap Tindak Pidana Peretasan Data Bank di Indonesia, Jurnal Penelitian Hukum dan Kriminologi, 12 (1),.

Marzuki, P.M. (2017). Penelitian Hukum. Edisi Revisi Kencana, Jakarta.

Nastiti, P.W., & Wulandari, D. (2021). Menangani Peretasan Data dalam Perspektif Hukum Perlindungan Data Pribadi di Indonesia, Jurnal Dinamika Hukum.

Nurul Qamar et.al, (2017). Metode Penelitian Hukum (Legal Research Methods). Social Politic Genius, Makassar.

Permen Kominfo No 20/2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

PP No 71/2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Prasetiyo & Zuhdi, M. (2020). Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) Di Wilayah Hukum Poida DIY, 1 (2), 2020.

Ratulangi, C.H. (2021). Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan. Lex Privatum.

Sadli, S. (1976). Persepdi Sosial Mengenai Prilaku Menyimpang. Bulan Bintang, Jakarta.

Saleh, A.R. (2021) Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana, HUMKY: Jurnal Hukum, 1 (1).

Sudarso. (1981). Hukum dan Hukum Pidana. Bandung

Sumadi, H. (2015). Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia, Jurnal Wawasan Hukum, 3 (2),.

Sumber Peraturan Perundang-Undangan: Kitab Undang-Undang Hukum Pidana (KUHP);

UU No 14/2008 Tentang Keterbukaan Informasi Publik

UU No 19/2016 Tentang Informasi dan Tranksaksi Elektronik

UU No 24/2013 Tentang Perubahan atau Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

Widianto, A.P., & Rofiq, A. (2019). Kerjasama Internasional Dalam Penanggulangan Tindak Pidana Peretasan Data. Jurnal Legislasi Indonesia, 16 (2).

Winarto, Y. 10 Oktober 2023. Kasus Peretasan Data Bank Syariah Indonesia (BSI), Bareskrim Masuk Penyidikan, Kompas.com