Aghniya: Jurnal Ekonomi Islam
ISSN 2656-5633 (Online)
Vol. 4, No. 2 (2022)

Studi Literatur Kejahatan Siber Pada Sistem Perbankan Syariah Di Era 4.0

Khairrun Nisa[1*], Chairina[2]

[*1,2]*Universitas Islam Negeri Sumatera Utara*
[*1]*email: khairrunnisa042@gmail.com*
[2]*email: chairina@uinsu.ac.id*

Keywords:
Cyber, banking, crime, development.

ABSTRACT

Electronic technology is growing at the same rate as the number of crimes, from the traditional to those using expertise in electronic technology for their own benefit or that of others. This study aims to determine whether the rapid development of technology has caused negative excesses, including the growth of a more sophisticated type of crime known as cybercrime and the use of sophisticated information technology and computers by criminals in banking for the purpose of stealing card data and customer money. The author analyzed previous research using a literature review approach in this study. Various Islamic banking crimes in Indonesia can be learned from the findings of this study.

Keywords:
Siber, perbankan, kejahatan, perkembangan.

ABSTRAK

Teknologi elektronik tumbuh dengan kecepatan yang sama dengan jumlah kejahatan, dari yang tradisional hingga yang menggunakan keahlian dalam teknologi elektronik untuk keuntungan mereka sendiri atau orang lain. Penelitian ini bertujuan untuk mengetahui apakah perkembangan teknologi yang pesat telah menimbulkan ekses negatif antara lain tumbuhnya jenis kejahatan yang lebih canggih yang dikenal dengan cybercrime dan penggunaan teknologi informasi dan komputer yang canggih oleh penjahat di perbankan untuk tujuan pencurian data kartu dan uang pelanggan. Penulis menganalisis penelitian terdahulu dengan menggunakan pendekatan literature review dalam penelitian ini. Berbagai kejahatan perbankan syariah di Indonesia dapat dipelajari dari temuan penelitian ini.

A. Pendahuluan

Ukuran untuk menentukan apakah suatu perilaku yang mencakup semua aspek kehidupan modern berhasil atau tidak adalah kemajuan teknologi informasi saat ini. Internet dapat digunakan untuk berbagai aktivitas, termasuk transaksi perbankan(Kevin Yoga Prasetyo, Fatika Damayanti, Abdul Basith, Meri Wiji Utami, Reza Fitra Abdillah, 2021). Sebagai lembaga ekonomi, bank melakukan dua hal utama, yaitu mengambil uang dari masyarakat dalam bentuk tabungan dan menyalurkannya kepada masyarakat dalam bentuk kredit atau bentuk lainnya untuk meningkatkan taraf hidup masyarakat. Bank

ISSN 2656-5633 (Online)
Vol. 4, No. 2 (2022)

memiliki kedudukan yang membuatnya rentan terhadap penyalahgunaan wewenang, baik oleh bank itu sendiri maupun oleh pihak luar yang memanfaatkan bank sebagai tempat persembunyian hasil kejahatannya. Bank mengedarkan uang, namun terdapat aktivitas perbankan yang melampaui atau melanggar peraturan yang berlaku karena alasan tertentu. Hal semacam ini dikenal dengan kejahatan perbankan.(Sulisrudatin, 2014).

Kemampuan sistem keamanan untuk menjalankan fungsinya masing-masing terkait dengan berbagai kejahatan terkait perbankan yang dapat dilakukan. Infrastruktur yang dikembangkan hingga saat ini dan sistem keamanan sama-sama terhubung dengan sumber daya manusia. Penipuan perbankan dimulai dengan kemajuan manusia dalam sains dan teknologi dan tumbuh bersama mereka. Kejahatan ini dianggap sebagai kelas "elit". Karena tidak semua orang mampu, maka disebut sebagai “elit”. Kejahatan kelas "elit" ini tidak membutuhkan banyak usaha untuk dilakukan. Kapasitas untuk berpikir merupakan faktor penting dalam mencapai berbagai hasil. Bentuk dan pola kejahatan yang akan muncul ke permukaan akan lebih banyak dipengaruhi oleh tingkat perkembangan peradaban manusia. Akibatnya, ketika komputer tersebar luas di seluruh dunia, orang menjadi disibukkan dan diganggu oleh efek negatif yang ditimbulkannya, seperti kejahatan komputer *(cybercrime)*(Laksono et al., 2022).

Namun, pada intinya istilah *“cybercrime”* mengacu pada setiap kejahatan yang melibatkan komputer atau dunia maya(Situmeang, 2021). Pada dasarnya, cybercrime adalah istilah yang menyinggung kejahatan dengan komputer atau jaringan komputer sebagai perangkat, target, atau tempat terjadinya kesalahan. Cek penipuan, penipuan kartu kredit *(carding)*, penipuan kepercayaan, penipuan identitas, pornografi anak, dan bentuk penipuan lainnya termasuk dalam kategori ini. Menurut (Alhakim & Sofia, 2021) istilah *"cybercrime"* mengacu pada aktivitas apa pun yang terjadi secara online atau melalui penggunaan komputer. Namun, seperti disebutkan sebelumnya, istilah "kejahatan dunia maya" mengacu pada jenis aktivitas kriminal tertentu yang terjadi di dunia maya dan melibatkan ancaman yang melibatkan komputer(Arofah & Priatnasari, 2020).

Ada beberapa penelitian yang membahas tentang *cybercrime* di perbankan. Salah satu studi tersebut mengatakan bahwa masalah yang mengarah pada kejahatan di perbankan adalah pengguna tidak cukup waspada untuk melindungi informasi pribadi. Peneliti menyarankan penerapan teknik pencegahan *kriptografi*, *biometrik*, dan *phishing*, yang diantisipasi dapat melindungi pengguna dari kejahatan di sektor perbankan, sebagai sarana untuk mengatasi masalah ini(Ratulangi, 2021).

ISSN 2656-5633 (Online)
Vol. 4, No. 2 (2022)

Penjahat dunia maya menargetkan pasar terbesar di Indonesia. Pada Walk 2020 tepatnya diambil informasi klien Tokopedia dan diduga programmernya berasal dari Pakistan (Mukaromah, 2020). Penemuan bahwa seseorang menjual 91 juta catatan Tokopedia di web gelap seharga US$ 5.000, atau sekitar 74 juta, menandakan dimulainya informasi peretasan (Aldin, 2020). Selain itu, 279 juta nama, alamat, nomor telepon, dan jumlah gaji milik warga negara Indonesia telah diretas dan dijual di *Raid Forums* hingga tahun 2021. *Cybercrime* memiliki berbagai bentuk dan selalu berubah. Dalam industri perbankan, layanan perbankan elektronik meliputi *skimming, malware,* dan *hacking* dengan menggunakan akses internet untuk bertransaksi, yang kemudian dimanfaatkan oleh para pelaku kejahatan siber. Bank menggunakan layanan *Electronic Banking* (E-banking) untuk menyediakan informasi perbankan dan layanan transaksi kepada nasabah, sehingga nasabah dapat dengan mudah melakukan berbagai transaksi perbankan melalui internet. Misalnya, pengecekan saldo deposito, pembelian, pembayaran tagihan, transfer dana antar bank, pembukaan rekening baru, dan transaksi perbankan lainnya. Perubahan strategi bisnis perbankan pelaku usaha sebagai terobosan baru dalam penerapan teknologi informasi hingga terciptanya produk-produk sektor perbankan. Selain itu, industri perbankan Indonesia disebut sebagai *"Agent of Development"* karena kontribusinya yang signifikan terhadap pertumbuhan, pemerataan, dan stabilitas ekonomi negara.(Ayunda & Rusdianto, 2021; Ekawati, 2018; Marufah et al., 2020).

Oleh karena itu, peneliti percaya bahwa tinjauan literatur yang berfokus pada kejahatan terkait perbankan syariah sangat penting. Hasil penelitian ini akan mengungkap kejahatan perbankan syariah yang spesifik di Indonesia. Penelitian ini diyakini penting agar dapat menjadi bahan evaluasi bagi pihak kepolisian dan perbankan syariah dalam penciptaan strategi untuk menekan tindak kriminal di perbankan syariah Indonesia.

B. Metode Penelitian

Pendekatan kualitatif berdasarkan wawancara pustaka, yaitu melakukan kajian berdasarkan berbagai bacaan, antara lain jurnal, buku, peraturan perundang-undangan, dan tulisan – tulisan ilmiah. Studi penulisan yang dilakukan dalam penelitian ini merupakan suatu bentuk penelitian yang dilakukan dengan mengumpulkan artikel jurnal dengan tema sesuai dengan tujuan penelitian, yaitu kejahatan siber dalam bidang perbankan syariah di era 4.0.

ISSN 2656-5633 (Online)
Vol. 4, No. 2 (2022)

Tujuan dari Teknik Studi Literatur ini adalah untuk menyediakan bahan referensi untuk membahas hasil penelitian dengan mengungkap berbagai teori dan temuan yang relevan. Urutan struktural tematik digunakan untuk pengumpulan data kajian literatur dalam penelitian ini dengan cara mengelompokkan dan mendiskusikan sumber sesuai dengan tema atau topik. Pembahasan dalam penelitian ini dapat diperkuat dengan mengelompokkan tema atau topik penelitian. Pengumpulan tinjauan literatur melibatkan beberapa langkah, termasuk mencari artikel yang terkait dengan masalah dalam beberapa cara, memilah struktur penjelas, dan membandingkan data yang terkait satu sama lain berdasarkan konten artikel yang relevan dengan topic tujuan studi ini.

C. Hasil Dan Pembahasan

Menurut Potabuga (2019), peran bank sebagai badan usaha adalah sebagai perantara keuangan *(Financial Intermediary)*. Peran ini melibatkan penerimaan dana *(funding)* dari individu yang memiliki kelebihan dana dan menyalurkan dana tersebut kepada pengguna dalam bentuk kredit. "Hubungan fidusia" adalah hubungan berbasis kepercayaan antara bank dan deposan. Bisa dipastikan industri perbankan akan gagal jika tidak mendapat kepercayaan dari nasabahnya. Oleh karena itu, untuk mendapatkan kepercayaan masyarakat, bank harus menjaga tingkat kesehatan bank pada tingkat yang konstan(Kurniawan & Hapsari, 2021).

Pesatnya penyebaran teknologi informasi berdampak pada sejumlah aktivitas manusia, termasuk perbankan, seperti yang telah disebutkan sebelumnya. Pesatnya pertumbuhan teknologi informasi dengan tujuan mempermudah aktivitas manusia. Dalam perkembangan teknologi informasi di sektor perbankan, efisiensi dan efektivitas memegang peranan penting. Dalam industri perbankan, bentuk efektif teknologi informasi yang dikenal sebagai *electronic banking* (E-banking) menempatkan fasilitas layanan perbankan dalam genggaman. Namun, ada risiko penggunaan data pelanggan secara ilegal melalui kejahatan dunia maya di balik kemudahan ini. Oleh karena itu, untuk menjaga kepercayaan masyarakat terhadap kemampuan industri perbankan dalam memanfaatkan teknologi informasi, pelaku usaha harus dilengkapi dengan pengamanan yang memadai. Namun demikian, instrumen hukum juga harus dapat memberikan rasa aman bagi nasabah industri perbankan.

Maraknya kejahatan dunia maya akan selalu berkorelasi langsung dengan kecanggihan suatu teknologi. Sehingga kejahatan dunia maya akan selalu diikuti dengan

ISSN 2656-5633 (Online)
Vol. 4, No. 2 (2022)

kejahatan jenis baru. *Hacking*, *cracking*, *carding* sampai *probe*, pemindaian, akun yang dikompromikan, kompromi *root*, penolakan layanan, dan penyalahgunaan nama domain hanyalah beberapa bentuk kejahatan dunia maya saat ini (Angelina, 2022).

Penjahat dunia maya di industri perbankan sering menggunakan strategi berbasis teknologi informasi berikut :

a. *Skimming*, khususnya suatu bentuk kejahatan dunia maya di mana informasi nasabah dicuri saat menggunakan ATM untuk bertransaksi,
b. *Malware* (*malicious software*), yakni perangkat lunak berbahaya yang dirancang untuk merusak sistem dan perangkat komputer serta mencuri data,
c. *Hacking*, yakni jenis kejahatan dunia maya di mana program komputer diserang dan komputer milik individu atau bisnis pribadi dieksploitasi untuk tujuan ilegal atau untuk keuntungan orang lain.

Phishing merupakan salah satu metode yang digunakan dalam pola penyerangan yang menitik beratkan pada serangan terhadap pengguna internet atau pelanggan yang melakukan bisnis secara online. Dengan memotong jalur data dan kemudian mengganti data tersebut dengan informasi palsu, teknik phishing digunakan untuk membobol jaringan. Selain itu, dengan mengirimkan data terinfeksi ke email korban, cara ini juga bisa digunakan untuk mengirimkan malware..

Bank dapat menggunakan autentikasi 2 faktor untuk mencegah hal tersebut, khususnya untuk memvalidasi data atau informasi nasabah. Kata sandi dan token seperti kartu pintar digunakan untuk dua metode otentikasi. Namun, menambahkan prosedur validasi biometrik untuk memastikan keamanan pelanggan direkomendasikan untuk keamanan yang lebih baik(Widayanti, 2022).

Naam (2020) secara khusus menyelidiki bagaimana mengidentifikasi jalur kerja dan jenis malware untuk melindungi diri dari serangan malware. Penelitiannya berfokus pada bagaimana memerangi efek infeksi malware pada sistem komputer dengan memeriksa berbagai jenis dan cara kerja *malware* dan menentukan tindakan terbaik.

Simon & Anderson (2021) menyelidiki penggunaan teknik *skimming* kamera dan *mikrofon* untuk mendapatkan PIN pada smartphone. Sistem operasi berbasis Android pada smartphone Nexus S dan Galaxy S3 berfungsi sebagai platform pengujian untuk metode ini. Tujuan dari penelitian ini adalah untuk menguji sistem keamanan smartphone terhadap pencurian PIN berbasis skimming.

Azhar (2018) mengembangkan prototipe aplikasi yang diharapkan mampu memberikan notifikasi berupa aktivitas transaksi yang dilakukan oleh pengguna melalui mobile banking guna mengetahui cara mendeteksi peretasan pada mobile banking. Pengguna memiliki opsi untuk menentukan apakah pemberitahuan itu palsu setelah menerimanya.

D. Kesimpulan

Di satu sisi, perkembangan teknologi informasi di industri perbankan memudahkan industri perbankan dan nasabahnya. Namun di sisi lain, risiko *cybercrime* yang dapat merugikan nasabah secara finansial dapat muncul. Agar selalu dapat menjaga kepercayaan masyarakat, industri perbankan jasa keuangan yang berlandaskan asas kepercayaan masyarakat harus terus meningkatkan keamanan siber.

Menurut penelitian terkait, ada sejumlah opsi untuk menyelesaikan masalah ini, salah satunya adalah menerapkan otentikasi tiga kali lipat, yang memerlukan penggunaan biometrik, token, dan kata sandi. Big data juga dapat digunakan oleh keamanan untuk memproses transaksi keuangan yang tidak adil.

E. Daftar Pustaka

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*.

Angelina, V. (2022). *Analisis Yurisdiksi Cyberlaw di Indonesia dalam Penanganan Kasus Cybercrime yang Merugikan Nasabah Bank Pengguna Fitur Internet Banking*. repository.uib.ac.id.

Arofah, N. R., & Priatnasari, Y. (2020). Internet Banking Dan Cyber Crime: Sebuah Studi Kasus Di Perbankan Nasional. *Jurnal Pendidikan Akuntansi Indonesia*.

Ayunda, R., & Rusdianto, R. (2021). Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence dalam Aktifitas Perbankan di Indonesia. *Jurnal Komunikasi Hukum (JKH)*.

Ekawati, D. (2018). Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan. *UNES Law Review*.

Kevin Yoga Prasetyo, Fatika Damayanti, Abdul Basith, Meri Wiji Utami, Reza Fitra Abdillah, K. (2021). Pengaruh e-commerce terhadap tindak kejahatan siber di era milenium untuk generasi milenial. *Journal of Education and Technology*, *1*(1), 1–6.

Kurniawan, K. D., & Hapsari, D. R. I. (2021). Kejahatan Dunia Maya Pada Sektor

ISSN 2656-5633 (Online)
Vol. 4, No. 2 (2022)

Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah. *Pleno Jure Jurnal Ilmu Hukum*.

Laksono, H. D., Prabowo, I. H., & Budhi, A. S. (2022). OPTIMALISASI PERLINDUNGAN KONSUMEN PERBANKAN BEDASARKAN UU NO 8 TAHUN 1999. *Prosiding HUBISINTEK*.

Marufah, N., Rahmat, H. K., & ... (2020). Degradasi Moral sebagai Dampak Kejahatan Siber pada Generasi Millenial di Indonesia. *… Jurnal Ilmu Pengetahuan …*.

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

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*.

Sulisrudatin, N. (2014). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara*, *9*(1), 26–39. https://doi.org/10.35968/jh.v9i1.296

Widayanti, P. W. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. *Legacy: Jurnal Hukum Dan …*.