DATIN LAW JURNAL
Volume. 5 Nomor. 2 Desember 2024. ISSN 2722-9262
http://dx.doi.org/10.36355/dlj.v1i1
Open Access at: https://ojs.umb-bungo.ac.id/index.php/DATIN/index

Peran Digital Forensik Terhadap Pencurian Data Pribadi Di Sektor Perbankan Digital

Dewi Maesyaroh[1]
Fakultas Hukum, Universitas Sebelas Maret
Jalan Ir. Sutami 36 A, Kentingan Surakarta, Jawa Tengah, 57126
Telp : 0852-2600-3036 E-mail : dewimaesyaroh8@gmail.com

ABSTRACT

Digital Forensics is a discipline that deals with the collection, analysis, interpretation, and presentation of digital evidence (such as electronic data, files, logs, and other digital traces) within the context of legal or security investigations. The research issues encompass two main aspects. Firstly, it involves exploring the legal foundations governing the field of digital forensics. Secondly, it investigates the role of digital forensics in cases of personal data theft within the banking sector. The research employs a normative juridical method with a legal approach and a conceptual approach. It includes case studies and analyses of data theft incidents targeting several prominent digital banks. Through the analysis of digital evidence, the research discusses the techniques and methodologies of digital forensics applied to detect incidents, reconstruct events, and collect evidence for use in legal proceedings. The objective is to uncover cybercrime, identify perpetrators, and conduct forensic investigations into attacks within the digital banking environment. The findings indicate the role of digital forensics in enhancing the security of banking systems by identifying potential security vulnerabilities and formulating preventive measures to protect customers' personal data. The research also provides crucial insights for banking institutions and law enforcement experts to bolster their resilience against threats of personal data theft in the digital banking era.

Keywords: Digital Forensics, Personal Data Theft, Digital Banking.

ABSTRAK

Digital Forensik adalah suatu disiplin ilmu yang berkaitan dengan pengumpulan, analisis, interpretasi, dan presentasi bukti digital (seperti data elektronik, file, log, dan jejak digital lainnya) dalam bidang investigasi hukum atau keamanan. Permasalahan penelitian ini mencakup dua aspek utama. Pertama, mencari dasar hukum yang mengatur bidang digital forensik. Kedua, menyelidiki peran digital forensik dalam kasus pencurian data pribadi di sektor perbankan. Metode yang digunakan dalam penelitian ini adalah metode yuridis normatif dengan pendekatan undang-undang, dan pendekatan konseptual. Penelitian ini juga melibatkan studi kasus dan analisis terhadap pencurian data yang menyerang beberapa bank digital terkemuka. Melalui analisis bukti digital, penelitian ini membahas teknik dan metodologi forensik digital yang diterapkan untuk mendeteksi insiden, merekonstruksi kejadian, dan mengumpulkan bukti yang dapat digunakan dalam proses hukum. Tujuannya adalah pada pengungkapan kejahatan cyber, identifikasi pelaku, dan penyelidikan forensik terhadap serangan yang terjadi di lingkungan perbankan digital. Hasil penelitian menunjukkan peran forensik digital dalam meningkatkan keamanan sistem perbankan, dengan mengidentifikasi potensi kelemahan keamanan dan menyusun langkah-langkah pencegahan untuk melindungi data pribadi nasabah. Penelitian juga dapat memberikan saran bagi lembaga perbankan dan penegak hukum untuk meningkatkan ketahanan mereka terhadap ancaman pencurian data pribadi di era perbankan digital.

Kata Kunci: Digital Forensik, Pencurian Data Pribadi, Perbankan Digital.

[1] Mahasiswa Fakultas Hukum Universitas Sebelas Maret

PENDAHULUAN

Era transformasi digital yang berkembang pesat, memberi dampak positif terhadap perkembangan disektor perbankan yaitu dengan munculnya perbankan digital. Perbankan digital telah menjadi pilar utama dalam menyediakan layanan keuangan yang inovatif dan mudah diakses. Kemajuan teknologi digital telah mengubah sektor industri dan layanan keuangan saat ini. Munculnya bank digital dipicu oleh perkembangan teknologi digital, khususnya, dan didorong oleh kebutuhan masyarakat akan kemudahan dan efisiensi dalam mengakses layanan keuangan.[2] Dengan bank digital, proses transaksi keuangan menjadi lebih praktis melalui aplikasi atau platform teknologi, membawa perubahan dalam gaya hidup dan perilaku masyarakat sebagai konsumen karena kenyamanan yang ditawarkan. [3] Perkembangan era digital mempermudah akses nasabah terhadap layanan keuangan melalui perangkat genggam. Dengan ini, nasabah dapat dengan mudah melakukan transaksi perbankan menggunakan berbagai metode, seperti layanan pesan singkat (SMS) banking hingga internet banking, tanpa harus mengunjungi fisik kantor cabang. Keleluasaan ini memungkinkan nasabah untuk mengakses layanan perbankan melalui aplikasi yang disediakan oleh masing-masing bank [4].

Penggunaan aplikasi perbankan digital dan penyimpanan data secara elektronik membuka peluang baru bagi potensi risiko keamanan, seperti akses tidak sah, pencurian identitas, dan penyalahgunaan informasi pribadi. Oleh karena itu, kerangka yuridis harus memastikan bahwa perbankan digital mematuhi standar keamanan data yang ditetapkan oleh hukum untuk melindungi privasi dan keamanan nasabah. Dalam konteks ini, regulasi yang ketat dan peraturan perlindungan data menjadi dasar hukum yang mendukung perlindungan nasabah terhadap ancaman pencurian data pribadi di platform perbankan digital.

Dampak positif bank digital sangat besar bagi berbagai pihak, termasuk konsumen, penyelenggara, dan pemerintah. Konsumen dapat menikmati system perbankan digital layanan yang lebih baik, penyelenggara bank digital dapat mengurangi biaya modal dan operasional, sementara pemerintah dapat mendorong akses keuangan yang merata dan inklusif.[5] Fenomena ini memberikan dampak positif bagi efisiensi transaksi dan kenyamanan nasabah, namun timbul pula kekhawatiran serius terkait dengan perlindungan data nasabah terutama terkait dengan isu perlindungan data pribadi. Maraknya insiden ini menimbulkan kekhawatiran bahwa kepercayaan masyarakat terhadap layanan bank digital yang disediakan akan mengalami penurunan. Keamanan berpengaruh terhadap niat untuk bertransaksi online. [6]

---

[2] Inda Rahadiyan, "Perkembangan Financial Technology Di Indonesia Dan Tantangan Pengaturan Yang Dihadapi," *Artificial Intelligence and the Law* (2020): 31–48.

[3] H S Disemadi et al., "Literasi Masyarakat Pesisir Terhadap Perlindungan Data Pribadi Dalam Transaksi Financial Technology," *Jurnal Abdimasa …* 5, no. 2 (2022): 68–76, https://unimuda.e-journal.id/jurnalabdimasa/article/view/2504%0Ahttps://unimuda.e-journal.id/jurnalabdimasa/article/download/2504/1109.

[4] Melia Prabangasta Yustisia, "PERLINDUNGAN BAGI NASABAH DALAM PENYELENGGARAAN LAYANAN PERBANKAN DIGITAL DI INDONESIA," *Program Magister Hukum FHUI* 1, no. July (2022): 24, https://scholarhub.ui.ac.id/dharmasisyaAvailableat:https://scholarhub.ui.ac.id/dharmasisya/vol1/iss4/24.

[5] Ida Martinelli, "Menilik Financial Technology (Fintech) Dalam Bidang Perbankan Yang Dapat Merugikan Konsumen," *Jurnal SOMASI (Sosial Humaniora Komunikasi)* 2, no. 1 (2021): 32–43.

[6] E. Purnamasari, A. A. Bakri, and E. C. Mayndarto, "The Impact of Privacy, Security, And Trust on Online Transaction Intentions at Bank BCA Bandung,"

Digital Forensik ialah penerapan ilmu pengetahuan dan teknologi komputer dalam konteks pembuktian hukum. Tujuan utama dari digital forensik ini adalah untuk membuktikan kejahatan yang terkait dengan teknologi tinggi atau kejahatan komputer secara ilmiah. Hal ini dilakukan melalui proses pengumpulan bukti digital yang dapat digunakan sebagai dasar untuk menjerat pelaku kejahatan tersebut. Pencarian bukti digital untuk menangkap pelaku sering kali merupakan tugas yang sangat rumit, memerlukan keahlian seorang analis/investigator forensik digital untuk mengikuti prosedur-prosedur yang diakui secara hukum, baik di tingkat nasional maupun internasional. Selain itu, mereka juga harus memiliki pemahaman teoritis yang mendalam terkait dengan bukti digital yang ditemukan, serta memiliki pengetahuan dalam penggunaan perangkat lunak forensik untuk mengidentifikasi bukti digital dengan benar.[7]

Digital forensik, sebagai disiplin ilmu, menitikberatkan pada penggunaan metodologi ilmiah untuk mengumpulkan, menganalisis, dan mengevaluasi bukti digital. Konsep ini mencakup prinsip-prinsip penelusuran digital dan pemulihan data elektronik, yang keduanya memegang peran sentral dalam menangani kejahatan berbasis teknologi, terutama di sektor perbankan digital. Peran digital forensik dalam penanganan keamanan data juga akan dipaparkan, mencakup teknik-teknik forensik digital, prosedur penyelidikan, dan penggunaan alat-alat forensik yang relevan. Ini memberikan gambaran tentang bagaimana forensik digital dapat mendeteksi, mencegah, dan merespons serangan siber di lingkungan perbankan digital. Kajian ini tidak hanya membangun landasan teoritis yang mendalam, tetapi juga menjadi kerangka kerja yang esensial untuk melanjutkan penelitian lebih lanjut tentang peran digital forensik dalam mengatasi pencurian data pribadi di sektor perbankan digital.

Berdasarkan latar belakang diatas maka rumusan masalah penelitian ini yaitu (1) Apa Dasar Hukum Pengaturan Digital Forensik. (2) Bagaimanakah Peran Digital Forensik Dalam Pencurian Data Pribadi di Sektor Perbankan. Penelitian ini bertujuan untuk memahami peran digital forensik dalam mengatasi pencurian data pribadi di sektor perbankan digital, serta menganalisis dampaknya terhadap keamanan dan integritas informasi nasabah. Hasil penelitian ini diharapkan dapat memberikan wawasan yang mendalam bagi lembaga perbankan dalam meningkatkan strategi keamanan digital. Selain itu, hasil penelitian ini juga dapat menjadi dasar bagi pengembangan kebijakan yang lebih efektif dalam melawan ancaman pencurian data pribadi di sektor perbankan digital.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis normatif dengan pendekatan undang-undang, pendekatan konseptual dan studi kasus. Metode yuridis normatif digunakan untuk mendalami kerangka hukum yang mengatur keamanan siber dan perlindungan data dalam konteks transaksi perbankan digital. Pendekatan ini memungkinkan analisis terinci terhadap norma-norma hukum yang berlaku, menyoroti tanggung jawab dan kewajiban lembaga perbankan dalam menjaga keamanan data pribadi nasabah. Sebagai pelengkap, dilibatkan pendekatan konseptual untuk menggali dasar-dasar teoritis digital forensik dan menerjemahkannya ke dalam kerangka hukum yang relevan.

International Journal of Economics and Management Research 2, no. 1 (2023): 215–222.

[7] A Tatumpe, "Analisis Yuridis Digital Forensik Dalam Pembuktian Tindak Pidana Di Indonesia," *Journal Scientia De Lex* 7 (2019): 1–9, https://www.ejournal.unpi.ac.id/index.php/scientia/article/view/42%0Ahttps://www.ejournal.unpi.ac.id/index.php/scientia/article/download/42/35.

Penelitian mengadopsi suatu pendekatan metodologis yang komprehensif, menggabungkan elemen-elemen hukum untuk memahami peran digital forensik dalam menanggapi pencurian data pribadi di sektor perbankan digital. Penelitian ini juga mengeksplorasi studi kasus aktual terkait pencurian data di beberapa bank digital terkemuka. Melalui analisis mendalam terhadap kasus-kasus ini, penelitian berusaha mengidentifikasi aspek-aspek hukum yang terlibat dalam respons dan penanganan forensik digital terhadap pelanggaran keamanan data. Dengan demikian, menggabungkan unsur-unsur hukum normatif, analisis konseptual, dan studi kasus, memberikan gambaran holistik tentang kontribusi digital forensik dalam memitigasi dan merespons tantangan hukum yang muncul seiring dengan pencurian data pribadi di sektor perbankan digital.

PEMBAHASAN DAN ANALISIS

A. Dasar Hukum Pengaturan Digital Forensik

Dalam bahasa Inggris istilah *forensic* berarti yang berhubungan dengan kehakiman atau peradilan. Istilah *forensic* digunakan untuk mengungkap bukti-bukti yang relevan dalam konteks kasus peradilan. Apabila istilah ini digabungkan dengan digital maka merujuk pada sesuatu yang terkait dengan komputer atau teknologi informasi, maka digital forensic atau forensik digital dapat didefinisikan sebagai ilmu dan keahlian yang berkaitan dengan identifikasi, pengumpulan, analisis, dan pengujian bukti digital yang menjadi objek penanganan dalam konteks kasus hukum.[8] Digital forensik adalah suatu rangkaian kegiatan penyelidikan yang dilaksanakan dengan maksud untuk mengidentifikasi serta mengumpulkan bukti-bukti digital guna memperkuat jejak-jejak fisik yang telah ada dalam suatu kasus yang tengah diselidiki.

Model penemuan digital forensik melalui 4 tahapan yaitu terdiri dari tahap mulai dari pengumpulan (*collection*), tahap pemeriksaan (*examination*), tahap analisis (*analysis*), dan tahap pelaporan (*reporting*). Kemudian dilakukan proses *Chain of Custody* yang bertujuan untuk merekam kronologi pengamanan, penahanan, pengendalian, dan pemindahan barang bukti fisik atau elektronik. *Chain of Custody* berperan dalam menyajikan urutan kronologis penanganan barang bukti, sehingga proses ini dapat dipertanggungjawabkan untuk kepentingan proses pengadilan.[9]

Undang-Undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang kemudian mengalami perubahan dengan UU Nomor 19 Tahun 2016 mengatur mengenai *cybercrime* juga diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang merupakan upaya pemerintah untuk melindungi masyarakat dalam konteks informasi dan transaksi elektronik termasuk kejahatan cyber dibidang perbankan digital. Keberadaan regulasi ini juga dianggap sebagai solusi dan pengakuan terhadap fakta bahwa alat bukti elektronik dapat dijadikan sebagai alat bukti yang sah, sebagaimana dijabarkan dalam Pasal 5 UU ITE menegaskan bahwa informasi atau dokumen yang disampaikan melalui sistem elektronik memiliki kekuatan hukum yang setara

[8] B. Givan, R. Wirawan, D. Andriawan, N. Aisyah, and A. S. Putra, "Effect of Ease And Trustworthiness To Use E-Commerce for Purchasing Goods Online," *International Journal of Educational Research & Social Sciences (IJERSC)* 2, no. 2 (2021): 277–282, cited in *Jurnal Esensi Infokom*, Vol. 6, No. 1, May 2022, p. 26.

[9] Nurul Aisyah et al., "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi dan Sistem Komputer* 6, no. 1 (2022): 22–27.

dengan informasi atau dokumen yang dibuat secara konvensional, kecuali ada ketentuan lain dalam peraturan perundang-undangan. Berdasarkan ketentuan pembuktian dalam KUHAP, ditegaskan bahwa alat penguji yang handal dan memadai diperlukan untuk menguji keabsahan alat bukti elektronik. Hal ini bertujuan agar alat bukti tersebut dapat diakui sah dalam proses litigasi, mematuhi persyaratan formil dan materiil.

Tujuan utama dari digital forensik adalah tidak hanya menemukan informasi yang bersifat digital, tetapi juga memastikan bahwa bukti fisik yang telah dikumpulkan sebelumnya dapat diperkuat dan diinterpretasikan melalui analisis bukti digital. Dengan kata lain, digital forensik berfungsi sebagai metode penyelidikan yang mendalam dan komprehensif untuk menyelidiki serta memvalidasi data digital dan fisik yang terkait dengan suatu kasus, dengan tujuan akhir membangun dasar bukti yang kuat dalam mendukung proses investigasi dan persidangan.

Digital forensik, pada dasarnya adalah bidang ilmu forensik yang secara khusus menitikberatkan pada penyelidikan serta identifikasi isi dari perangkat digital, yang sering kali terkait dengan kejahatan di ranah komputer. Meskipun istilah forensik digital pada awalnya digunakan secara bersamaan dengan forensik komputer, saat ini ruang lingkupnya telah berkembang secara signifikan, mencakup penyelidikan terhadap berbagai perangkat yang mampu menyimpan dan memproses data digital. Dengan kata lain, forensik digital melibatkan proses penemuan, analisis, dan interpretasi informasi digital untuk mendukung investigasi dan memperkuat bukti dalam berbagai konteks, termasuk kejahatan komputer.[10]

Digital forensik merupakan segmen forensik yang mengkaji dampak dan jejak sistem digital serta kemampuannya dalam meninggalkan data yang dapat diungkap kembali sebagai bukti dalam sistem yang sedang diselidiki.[11] Digital forensik bukan hanya menjadi instrumen penting untuk pengungkapan kejahatan berteknologi tinggi, tetapi juga sebagai alat proaktif yang dapat mendeteksi dan mencegah potensi ancaman keamanan data.

Peran digital forensik menjelma menjadi unsur utama dalam menjaga integralitas dan keamanan data pribadi di sektor perbankan digital yang terus berkembang. Digital forensik tidak sekadar berperan sebagai alat investigasi pasca-kejadian melainkan, ia menjadi tameng proaktif yang secara aktif berusaha mendeteksi, mencegah, dan merespons ancaman pencurian data sebelum potensi kerugian merambah. Di tengah dinamika serangan *cyber* yang semakin canggih dan kompleks, digital forensik menjadi fondasi strategis yang memberikan keunggulan dalam menghadapi tantangan perlindungan informasi sensitif nasabah. Pembuktian mengenai kebenaran atau ketidakbenaran

[10] A. Medikano, H. Ludiya, R. Wirawan, P. M. Akhirianto, S. Rachmawati, A. Sebayang, D. Efriyenty, R. Riko, I. Svinarky, B. J. Tama, and A. S. Putra, "Smart Transportation for Jakarta Smart City Residents," *International Conference on Global Optimization and Its Applications 2021*, vol. 1, no. 1 (2021): 21-21.

[11] Dewi, N. K., Irawan, B. H., Fitry, E., & Putra, A. S. (2020). "Konsep Aplikasi E-Dakwah Untuk Generasi Milenial Jakarta." IKRA-ITH INFORMATIKA: Jurnal Komputer dan Informatika, 5(2), 26-33.

terdakwa terhadap tindak pidana yang dituduhkan merupakan bagian yang sangat krusial dalam proses hukum pidana. Oleh karena itu, tujuan utama dari hukum acara pidana adalah mencari kebenaran substansial yang mendasar, yang menjadi inti dari proses pidana.

Keberadaan digital forensik tidak hanya mengandalkan respons terhadap serangan yang telah terjadi, tetapi lebih pada upaya pencegahan dan perlindungan yang proaktif. Dengan memanfaatkan pemahaman mendalam terhadap cara-cara serangan *cyber* berkembang, digital forensik mampu merinci dan menganalisis pola-pola serangan sekaligus mengidentifikasi potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pemahaman yang mendalam tentang dinamika serangan *cyber* memberikan digital forensik keunggulan strategis dalam memberikan perlindungan menyeluruh terhadap informasi nasabah. Digital forensik tidak hanya memberikan keamanan bagi individu nasabah, tetapi juga menjaga reputasi lembaga perbankan sebagai penyedia layanan yang andal dan bertanggung jawab di era digital.

Keamanan data telah menjadi aspek yang memerlukan perhatian lebih dalam dalam menjaga integritas informasi di era transformasi digital. Untuk menjawab tantangan tersebut, digital forensik muncul sebagai disiplin ilmu yang tidak hanya berfungsi sebagai alat investigasi, melainkan juga sebagai tameng proaktif dalam menjaga keamanan dan integritas data. Digital forensik dapat didefinisikan sebagai aplikasi ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum. Di era di mana teknologi terus berkembang, tantangan keamanan data, terutama terkait dengan data pribadi dan keuangan, semakin kompleks.

B. Peran Digital Forensik Dalam Pencurian Data Pribadi di Sektor Perbankan

Perlindungan terhadap data pribadi nasabah di sektor perbankan dilakukan oleh bank dengan mengacu pada prinsip kerahasiaan. Prinsip ini telah diatur dalam Undang-Undang Nomor 10 tahun 1998, yang secara tegas mengamanatkan bahwa bank memiliki kewajiban untuk menjaga kerahasiaan data pribadi nasabahnya. Artinya, bank harus menjaga kerahasiaan semua informasi terkait data dan informasi nasabah, termasuk informasi keuangan dan data pribadi. Regulasi ini dijelaskan dalam Undang-Undang Perbankan, di mana Pasal 1 ayat (28) mengartikan rahasia bank sebagai segala hal yang berkaitan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Secara lebih rigid perlindungan data pribadi nasabah perbankan diatur dalam Pasal 40 ayat (1) UU Perbankan kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44 dan Pasal 44A. Kendati hak konstitusional telah diakui, perlindungan data pribadi di Indonesia masih memerlukan perhatian serius untuk mengatasi risiko-risiko yang muncul di sektor perbankan digital.

Undang-Undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang kemudian mengalami

perubahan dengan UU Nomor 19 Tahun 2016 mengatur mengenai cybercrime juga diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang merupakan upaya pemerintah untuk melindungi masyarakat dalam konteks informasi dan transaksi elektronik termasuk kejahatan cyber dibidang perbankan digital. Keberadaan regulasi ini juga dianggap sebagai solusi dan pengakuan terhadap fakta bahwa alat bukti elektronik dapat dijadikan sebagai alat bukti yang sah, sebagaimana dijabarkan dalam Pasal 5 UU ITE menegaskan bahwa informasi atau dokumen yang disampaikan melalui sistem elektronik memiliki kekuatan hukum yang setara dengan informasi atau dokumen yang dibuat secara konvensional, kecuali ada ketentuan lain dalam peraturan perundang-undangan. Berdasarkan ketentuan pembuktian dalam KUHAP, ditegaskan bahwa alat penguji yang handal dan memadai diperlukan untuk menguji keabsahan alat bukti elektronik. Hal ini bertujuan agar alat bukti tersebut dapat diakui sah dalam proses litigasi, mematuhi persyaratan formil dan materiil.

Pencurian data pribadi yang terjadi di sektor perbankan merupakan ancaman serius yang dapat merugikan nasabah dan mengurangi kepercayaan publik terhadap lembaga keuangan. Dalam menghadapi tantangan ini, peran digital forensik muncul sebagai elemen kunci dalam menanggapi dan mencegah insiden pencurian data pribadi. Digital forensik dalam perbankan digital memiliki peran yang sangat penting untuk mengamankan informasi pribadi nasabah dan menjaga keamanan sistem perbankan secara keseluruhan. Digital forensik tidak hanya berperan sebagai alat investigasi setelah terjadinya pencurian data, tetapi juga sebagai upaya proaktif untuk mencegah pencurian data di masa depan. Metode yang dapat dilakukan ayitu analisis bukti digital, pemulihan data, dan rekonstruksi kejadian menjadi kunci utama dalam mengidentifikasi pelaku pencurian data kemudian menyusun strategi pencegahan yang lebih efektif.

Tujuan utama pembuktian digital forensik adalah untuk menyediakan bukti yang kuat dan dapat diandalkan untuk mendukung investigasi kriminal atau proses hukum dalam tindak pidana *cybercrime*. Dalam tindak pidana *cybercrime* bukti dibedakan menjadi dua jenis yaitu bukti elektronik dan bukti digital. Bukti elektronik dan bukti digital memiliki perbedaan yang penting. Bukti elektronik merujuk pada perangkat fisik seperti handphone, komputer, laptop, dan USB, sementara bukti digital merujuk pada konten yang terdapat dalam bukti elektronik tersebut.[12]

Pasal 183 menunjukkan bahwa sistem hukum acara yang berlaku cenderung mengikuti teori pembuktian yang bersifat negatif. Seorang individu hanya dapat dianggap bersalah jika setidaknya ada dua bukti yang sah, dan hakim memperoleh keyakinan bahwa terdakwa telah melakukan tindak pidana. Menurut Simons, hukuman didasarkan pada pembuktian ganda, yaitu melibatkan peraturan perundang-undangan dan keyakinan hakim. Sesuai dengan undang-undang, keyakinan hakim tersebut

[12] A. Wirara, B. Hardiawan, dan M. Salman, "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan 'WhatsApp'," eknoin Vol. 26, No. 1, Maret 2020, pp. 66-74, 2020.

harus didasarkan pada ketentuan yang tercantum dalam peraturan perundang-undangan.[13]

Dalam penanganan kasus pencurian data pribadi di sektor perbankan, peran hakim yang didasarkan pada prinsip-prinsip Kitab Undang-Undang Hukum Acara Pidana (KUHAP) sangat penting. Hakim, dalam memutus suatu perkara, terikat pada alat bukti yang diakui oleh KUHAP, sehingga hanya bukti yang sah dan sesuai dengan regulasi hukum yang dapat digunakan dalam menghadapi kasus pencurian data pribadi. Dalam pencurian data pribadi, hal ini memastikan bahwa bukti elektronik dan digital yang digunakan dalam kasus-kasus semacam itu diperlakukan secara hati-hati dan sesuai dengan standar yang telah ditetapkan.

Melalui penggunaan alat bukti yang sah dan proses peradilan yang berlandaskan hukum, hakim dapat memastikan perlindungan hak individu yang menjadi korban pencurian data pribadi. Keadilan dalam pengadilan bukan hanya bagi pelaku tindak pidana, tetapi juga bagi korban, memastikan bahwa hukuman yang diberikan sesuai dan bahwa hak-hak individu terlindungi dengan baik. Dengan demikian, peran hakim yang mengikuti prinsip-prinsip KUHAP dapat memberikan kontribusi positif dalam mengatasi kasus pencurian data pribadi di sektor perbankan, memastikan bahwa penanganan kasus dilakukan secara adil, transparan, dan sesuai dengan norma hukum yang berlaku.

Kejahatan siber termasuk pencurian data pribadi diperangkat lunak umumnya meninggalkan catatan aktivitas yang dapat dijadikan dasar pembuktian. Pembuktian digital forensik digital dalam kasus ini dapat berupa pengumpulan, analisis, interpretasi, dan penyajian bukti-bukti dalam suatu proses hukum dengan menggunakan metode ilmiah dan teknologi. Digital forensic dapat membantu investigator mencari bukti akurat dengan menghemat waktu dan usaha.[14] Langkah pertama yang diambil oleh seorang ahli adalah memeriksa apakah suatu sistem dapat dipercaya. Apabila sistem tersebut dapat dipercaya, secara otomatis data digital atau elektronik yang terdapat dalam komputer tersebut dapat dianggap dapat dipertanggungjawabkan dan dapat dijadikan alat bukti dengan kekuatan yang setara dengan alat bukti lain yang diakui oleh Pasal 184 KUHAP.[15]

Untuk memperoleh pemahaman tentang bentuk penyalahgunaan komputer dalam pencurian data pribadi di platform digital, berikut ini akan dijelaskan beberapa contoh kasus sebagai berikut:

- Pada tanggal 22 Juli 2023, diperkirakan sekitar 6,4 juta informasi pengguna kartu kredit BCA bocor dan diperjualbelikan di sebuah forum hacker. Informasi yang terungkap mencakup alamat, nomor telepon, dan data lainnya. Gambar tangkapan layar yang diunggah menunjukkan bahwa data tersebut dijual

[13] Martinus Jefry Clinton Purba, "Tindak Pidana Komputer Dan Upaya Pembuktian," *Lex Crimen* x, no. 4 (2021): 215–225.

[14] Nur Iman, Aris Susanto, and Rahmat Inggi, "Analisa Perkembangan Digital Forensik Dalam Penyelidikan Cybercrime Di Indonesia (Systematic Review)," *Jurnal Telekomunikasi dan Komputer* 9, no. 3 (2020): 186.

[15] Martinus Jefry Clinton Purba, "Tindak Pidana Komputer Dan Upaya Pembuktian."

di BreachForums, sebuah platform tempat hacker dari seluruh dunia dapat bertransaksi atau bahkan memberikan informasi hasil pembobolan secara gratis.[16]

- Pada bulan Mei 2023, terjadi Pencurian Data di Bank Syariah Indonesia oleh kelompok peretas asal Rusia yang dikenal sebagai Lockbit. Mereka mengklaim telah melumpuhkan salah satu server BSI, mengakibatkan tidak dapat diaksesnya aplikasi mobile banking oleh para nasabah. Akibatnya, BSI juga mengalami kerugian sebanyak 1,5 TB data, termasuk informasi pribadi dari nasabah dan karyawan. Kejadian ini dikategorikan sebagai ransomware karena Lockbit menuntut pembayaran sejumlah uang agar data tersebut tidak dijual di *dark web.*[17]

Melihat kasus tersebut digital forensik dapat membantu mengidentifikasi pelaku kejahatan, menganalisis data terinfeksi atau dicuri untuk memahami cara serangan terjadi, dan mengumpulkan bukti digital yang dapat digunakan di pengadilan. Selain itu, dengan memainkan peran proaktif, digital forensik juga dapat memberikan rekomendasi untuk meningkatkan keamanan serta menerapkan tindakan pencegahan guna mencegah terjadinya pencurian data pribadi di masa depan. Dengan keterlibatan digital forensik, sektor perbankan digital dapat mengejar peningkatan keamanan dan memberikan perlindungan yang lebih efektif terhadap informasi sensitif nasabah.

Selain itu, digital forensik juga berperan dalam mendeteksi pola serangan yang mungkin muncul di masa depan. Dengan memahami cara pelaku kejahatan cyber beroperasi, lembaga perbankan dapat meningkatkan kecerdasan keamanan mereka dan merespons lebih cepat terhadap ancaman potensial. Ini menciptakan siklus pembelajaran yang kontinu, di mana peningkatan keamanan didasarkan pada pengalaman dan pemahaman mendalam terhadap serangan sebelumnya.

Digital forensik menjadi alat utama untuk mengidentifikasi, menganalisis, dan mengumpulkan bukti terkait aktivitas penipuan. Seiring dengan kemajuan teknologi yang terus berkembang, para ahli digital forensik perlu terus meningkatkan keterampilan dan pengetahuan mereka agar tetap efektif dalam mengungkap kejahatan di era digital. Melalui kerja sama yang erat antara ahli digital forensik, lembaga penegak hukum, dan pihak berwenang lainnya, usaha untuk melawan penipuan di ranah digital dapat menjadi lebih efisien dan berhasil.

Dengan demikian, penggunaan digital forensik bukan hanya sebagai respons setelah terjadinya ancaman, tetapi juga sebagai alat yang proaktif untuk membentuk keamanan sistem perbankan secara menyeluruh. Dalam dunia perbankan digital yang terus berkembang, investasi dalam digital forensik menjadi langkah penting untuk menjaga kepercayaan nasabah dan

[16] 2 Kasus Siber Terkait BCA dalam Sepekan, Dugaan Bocor Data dan Virus," CNN Indonesia, diakses tanggal 1Januari2024,https://www.cnnindonesia.com/teknologi/20230727050921-192-978329/2-kasus-siber-terkait-bca-dalam-sepekan-dugaan-bocor-data-dan-virus.

[17]"Contoh Kasus Cyber Crime," Cloudeka, diakses tanggal1Januari2024,https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/.

menjaga integritas serta keamanan data pribadi.

KESIMPULAN

Dasar hukum pengaturan digital forensik terdapat Pasal 5 UU ITE menyatakan bahwa keberlakuan hukum informasi atau dokumen yang dikirimkan melalui sistem elektronik setara dengan informasi atau dokumen yang dibuat secara konvensional. Digital Forensik, sebuah disiplin ilmu yang berfokus pada identifikasi, pengumpulan, analisis, dan pengujian bukti digital dalam konteks hukum. Digital forensik tidak hanya menemukan informasi digital tetapi juga memastikan bukti fisik yang telah dikumpulkan diperkuat dan diinterpretasikan melalui analisis bukti digital. Tujuan utamanya adalah membangun dasar bukti yang kuat untuk mendukung investigasi dan persidangan. Selain berperan sebagai alat investigasi, digital forensik juga menjadi tameng proaktif dalam mendeteksi, mencegah, dan merespons ancaman keamanan data.

Pencurian data pribadi di sektor perbankan menjadi ancaman serius yang dapat merugikan nasabah dan merusak kepercayaan publik terhadap lembaga keuangan. Dalam menghadapi tantangan ini, peran digital forensik muncul sebagai elemen kunci dalam menanggapi dan mencegah insiden pencurian data pribadi. Fokus digital forensik pada pengamatan, analisis, dan pemulihan data digital membantu mengidentifikasi pelaku kejahatan, memahami cara serangan terjadi, dan mengumpulkan bukti digital yang kuat. Metode analisis bukti digital, pemulihan data, dan rekonstruksi kejadian menjadi kunci utama dalam mengidentifikasi pelaku pencurian data dan menyusun strategi pencegahan yang lebih efektif.

SARAN

Untuk mengatasi pencurian data pribadi di sektor perbankan, beberapa saran yang dapat diterapkan untuk memperkuat peran digital forensik. Pertama, perlu peningkatan kolaborasi antara lembaga perbankan, ahli digital forensik, dan pihak berwenang untuk meningkatkan kecepatan dan efektivitas dalam menangani insiden keamanan. Kedua, implementasi teknologi keamanan yang canggih dan pemantauan secara real-time dapat membantu mendeteksi potensi serangan dan merespons dengan cepat. Selanjutnya, lembaga perbankan perlu memperkuat kebijakan privasi dan keamanan data internal mereka, termasuk implementasi prosedur digital forensik yang lebih proaktif dalam mendeteksi celah keamanan.

UCAPAN TERIMAKASIH

Ucapan terima kasih yang tulus kepada Dr. Anita Zulfiani, S.H., M.Hum., atas kontribusinya yang luar biasa dalam pembuatan jurnal tidak hanya memberikan wawasan yang berharga terkait teknik penulisan jurnal, tetapi juga memberikan arahan yang sangat membantu dalam menyusun metodologi, analisis data, dan interpretasi hasil. Terima kasih atas dedikasi, keramahan dan kesediaannya untuk berbagi pengetahuan mendalam telah memberikan kontribusi yang besar terhadap kesuksesan penelitian ini.

DAFTAR KEPUSTAKAAN

Aisyah, Nurul, Arman Syah Putra, Safrizal Safrizal, V H Valentino, Zikriah Zikriah, Budhi Sriyono Prasetyo, Daru Susanti, and Nurhayati Nurhayati. "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review." Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi dan Sistem Komputer 6, no. 1 (2022): 22–27.

Disemadi, H S, N Z Silviani, D Jaya, and ... "Literasi Masyarakat Pesisir Terhadap Perlindungan Data Pribadi Dalam Transaksi Financial

Technology." Jurnal Abdimasa 5, no. 2 (2022): 68–76.

Iman, Nur, Aris Susanto, and Rahmat Inggi. "Analisa Perkembangan Digital Forensik Dalam Penyelidikan Cybercrime Di Indonesia (Systematic Review)." Jurnal Telekomunikasi dan Komputer 9, no. 3 (2020): 186.

Martinelli, Ida. "Menilik Financial Technology (Fintech) Dalam Bidang Perbankan Yang Dapat Merugikan Konsumen." Jurnal SOMASI (Sosial Humaniora Komunikasi) 2, no. 1 (2021): 32–43.

Martinus Jefry Clinton Purba. "Tindak Pidana Komputer Dan Upaya Pembuktian." Lex Crimen x, no. 4 (2021): 215–225.

Melia Prabangasta Yustisia. "PERLINDUNGAN BAGI NASABAH DALAM PENYELENGGARAAN LAYANAN PERBANKAN DIGITAL DI INDONESIA." Program Magister Hukum FHUI 1, no. July (2022): 24.

Rahadiyan, Inda. "Perkembangan Financial Technology Di Indonesia Dan Tantangan Pengaturan Yang Dihadapi." Artificial Intelligence and the Law (2020): 31–48.

Tatumpe, A. "Analisis Yuridis Digital Forensik Dalam Pembuktian Tindak Pidana Di Indonesia." Journal Scientia De Lex 7 (2019): 1–9.

Wirara, A., Hardiawan, B., & Salman, M. (2020). "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan 'WhatsApp'." eknoin Vol. 26, No. 1, Maret 2020, pp. 66-74.

"2 Kasus Siber Terkait BCA dalam Sepekan, Dugaan Bocor Data dan Virus." CNN Indonesia. Diakses 1 Januari 2024. Website :https://www.cnnindonesia.com/teknologi/20230727050921-192-978329/2-kasus-siber-terkait-bca-dalam-sepekan-dugaan-bocor-data-dan-virus.

"Contoh Kasus Cyber Crime." Cloudeka. Diakses 1 Januari2024.Website:https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/.